

Manuel d'installation et d'utilisation de la Cryptolib CPS



v5.1.2 du 09/07/2015



Manuel d'installation et d'utilisation de la Cryptolib CPS

« ASIP Santé / PUSC / PSCE »

Version 5.1.2 du 09/07/2015

Historique du document			
Version	Date	Auteur	Commentaires
5.0.9	12/09/2014	ASIP/PTS/PSCE	Java : blocage du plugin par Internet Explorer 11 Limitation Mac OS X 10.10 Utilisation certificats CPx avec BouncyCastle et limitations
5.0.10	12/11/2014	ASIP/PUSC/PSCE	- Précisions dans la présentation de la CPx - Sécurité : changement de code porteur - Sécurité : 18.2 Certificats et clés privées : 3 éléments - Corrections fichiers installés sous Windows - Utilisation avancée du GALSS : activation des traces en 3.40.01 - « Contacts » en 2 sous-parties - Prérequis matériels : USB CCID et listes - AT_0160 et AT_0170 - XPI et anti-malware - Choix de lecteur - ODI : gestion cache Java
5.1.0	02/03/2015	ASIP/PUSC/PSCE	- ODI v5 - liste des limitations CSP v5 - MSSanté Info Service - Cryptolib CPS v5.0.15 (Windows / CSP / Chrome 41)

Historique du document			
Version	Date	Auteur	Commentaires
5.1.1	08/04/2015	ASIP/PUSC/PSCE	- ODI v5 - Java: limitations Chrome 42+ / NPAPI - AT_0200: Cryptolib CPS v5.0.16 (Windows), 5.0.7 (Linux), 5.0.15 (Mac OS X) / PKCS#11 / unused-bit)
5.1.2	29/05/2015	ASIP/PUSC/PSCE	- MAJ contacts supports - AT210 : C# : régression CSP - AT220 : Windows 10 : Spartan/Edge - MAJ liens hypertextes

1 Références

Documents de référence				
N°	**Version**	**Date**	**Auteur**	**Document**
[0]	1.0.0	21/02/2011	ASIP Santé	Licence d'utilisation de la Cryptolib CPS
[1]	1.1.0	21/10/2013	ASIP Santé	Site intégrateurs
[2]	4.0.11	06/08/2013	ASIP Santé	Outil de Diagnostic et d'Installation
[3]	4.0.0	21/05/2013	ASIP Santé	Manuel d'utilisation de l'Outil de Diagnostic et d'Installation
[4]	1.9.0	01/10/2013	ASIP Santé	Tableau de compatibilité Cryptolib CPS
[5]	2.0.1	01/05/2011	ASIP Santé	Présentation de la carte CPS3
[6]	1.9.0	01/09/2014	ASIP Santé GIE SESAM-Vitale	GALSS 3.xx - Gestionnaire d'Accès aux Lecteurs Santé Social
[7]	1.4.2	24/11/2009	ASIP Santé GIE SESAM-Vitale	Spécifications coupleur avec contact pour lecteurs PC /SC dans le domaine santé - social
[8]	1.0.0	02/04/2013	ASIP Santé	Procédure de concessions des spécifications de la carte CPS3
[9]	3.5.0	22/02/2007	Microsoft	Command-Line Switches for the Microsoft Windows Installer Tool
[10]	1.0.0	31/10/2013	ASIP Santé	Note de publication Installation MSI Cryptolib CPS Version 5.0.8 32bits
[11]	1.0.0	31/10/2013	ASIP Santé	Note de publication Installation MSI Cryptolib CPS Version 5.0.8 64bits

Documents de référence				
N°	**Version**	**Date**	**Auteur**	**Document**
[12]	1.5.0	16/10/2013	ASIP Santé	Manuel de programmation de la Cryptolib CPS v5[1]
[13]	1.1.0	29/05/2011	ASIP Santé	Documentation programme d'exemple de la Cryptolib CPS v5[2]
[14]	1.0.1	10/10/2012	ASIP Santé	Spécifications externes PKCS#11 de la Cryptolib CPS v5[3]
[15]	1.0.0	23/01/2012	ASIP Santé	Carte CPS - Guide de référence de la carte CPS3
[16]	1.1.0	16/10/2013	ASIP Santé	Impacts de la migration Cryptolib CPS v4 vers la Cryptolib CPS v5[4]
[17]	2.5.3	17/10/2013	ASIP Santé	Guide de mise en œuvre d'un Smartcard logon avec une Carte de Professionnel de Santé (CPS)
[18]	1.0.2	02/04/2013	ASIP Santé	Guide de mise œuvre des profils itinérants
[19]	1.0.0	18/10/2013	ASIP Santé	Téléchargements logiciels esante.gouv.fr
[20]	1.0.0	26/09/2013	ASIP Santé	PGSSI-S Référentiel D Authentification des acteurs de Santé

[1] Nécessite un compte sur integrateurs-cps, s'adresser à editeurs@asipsante.fr

[2] Nécessite un compte sur integrateurs-cps, s'adresser à editeurs@asipsante.fr

[3] Nécessite un compte sur integrateurs-cps, s'adresser à editeurs@asipsante.fr

[4] Nécessite un compte sur integrateurs-cps, s'adresser à editeurs@asipsante.fr

Documents de référence				
N°	**Version**	**Date**	**Auteur**	**Document**
[21]		2011	ISO	**Standards "Identification cards — Integrated circuit(s) cards with contacts":** ISO/IEC 7816-1 Part 1: Physical characteristics ISO/IEC 7816-2 Part 2: Dimensions and location of the contacts ISO/IEC 7816-3 Part 3: Electrical interface and transmission protocols ISO/IEC 7816-4 Part 4: Organization, security and commands for interchange
[22]			ISO	**Standards "sans-contact":** ISO/IEC 14443-1 Part 1: Physical characteristics ISO/IEC 14443-2 Part 2: Radio frequency power and signal interface ISO/IEC 14443-3 Part 3: Initialization and anticollision ISO/IEC 14443-4 Part 4: Transmission protocol
[23]	1.0.1	21/03/2008	ACSIEL (ex. GIXEL)	EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS [IAS ECC]
[24]		2004	ISO	ISO/IEC 7816-15 Identification cards — Integrated circuit cards Part 15: Cryptographic information application
[25]	1.0.2	10/10/2012	ASIP Santé	Les données métier de la CPS3 Volets CPS2ter et IAS[5]
[26]	1.1	30/11/2011	ASIP Santé	IGC - CPS2ter Les certificats X.509 des cartes CPS2ter et CPS3.1 et les CRLs
[27]	0.0.3	12/09/2014	ASIP Santé	Guide de mise en œuvre et de la partie sans contact de la Carte CPS3

Tableau 1 : Documents de référence

[5] Nécessite un compte sur integrateurs-cps, s'adresser à editeurs@asipsante.fr

2 Résumé

Ce manuel documente l'installation et l'utilisation de la Cryptolib CPS (dans ses versions 4 et 5) diffusée par l'ASIP Santé **[0]**.

Ce manuel est mis à jour suite à la sortie de la **Cryptolib CPS v5**.

La **Cryptolib CPS v5** est un composant logiciel installé sur les postes de travail. Elle permet aux systèmes d'exploitation de tirer pleinement profit des fonctionnalités offertes par la carte CPS3 et notamment d'exploiter les fonctionnalités offertes par les volets IAS-ECC **[23]** (signature, authentification) et sans contact de cette carte.

Cette version de la Cryptolib CPS gère aussi les anciennes cartes CPS2ter qui ont normalement disparu du terrain à compter de **mars 2014**.

Ce document reflète l'évolution du poste de travail PS, qui est passé en quelques années :

- D'un modèle {mono-poste, mono-applicatif, connecté via une liaison spécialisée}
- à un modèle {réseau local multi-postes, avec des postes multi-applicatifs, connecté à Internet}

Il est destiné :

- aux usagers
    - d'ordinateurs Windows, Macintosh, ou Linux
    - équipés d'un lecteur de cartes à puces PSS ou PC/SC
    - souhaitant exploiter les fonctionnalités offertes par les cartes CPx
    - en direct ou au travers de logiciels professionnels
- aux administrateurs de parcs informatiques
    - ayant besoin de déployer la Cryptolib CPS sur leurs parcs de machines
    - afin de gérer des postes exploitant les fonctionnalités offertes par les cartes CPx
- aux intégrateurs
    - ayant besoin d'installer et de maitriser l'installation de la Cryptolib CPS
    - pour leurs propres développements matériels ou logiciels
- aux supports
    - des institutions ou des éditeurs
    - comme support de rédaction des procédures de niveaux 1 et 2

Ce document s'organise en quatre parties principales :

1. Un guide d'installation des bibliothèques cryptographiques « Cryptolib CPS » pour aider l'opérateur dans ses manipulations et ses choix de réponses et s'assurer du bon fonctionnement ultérieur.
2. Un guide de première utilisation simple illustrant une connexion sécurisée par carte CPx sur un serveur de test de l'ASIP Santé.
3. Une aide aux diagnostics sous forme de liste de contrôles de cette installation si des problèmes sont rencontrés.
4. Une présentation technique détaillée pour comprendre le détail des opérations réalisées et introduire les opérations d'utilisations avancées (cas des établissements, des intégrateurs et des éditeurs).

Les installations TSE/Citrix sont reportées en annexe:

1. elles nécessitent une bonne connaissance préalable de l'installation standard du poste de travail
2. elles se réfèrent activement aux ressources ou à des points de contrôle communs avec l'installation standard du poste de travail

La Cryptolib CPS v5 **64bit** est nécessaire sur les **systèmes 64bit**, qui se démocratisent.

Les spécificités de chaque système sont détaillées au cas par cas au sein de ces grandes parties.

3 Sommaire

4 Contacts

Ce document renvoie régulièrement aux différents supports impliqués dans le processus d'installation et d'utilisation du poste de travail PS.

4.1 Contacts Santé&Social

Les principales sources de support sont les suivantes:

Nom	Niveau	Rôle	Contact
Support Assurance Maladie	1	Support CDR, Espace pro	0 811 709 710 Support-technique-ps@cnamts.fr
Support GIE SESAM-Vitale	1	Support GALSS, PSS, API lecture Vitale, FSV	02 43 57 42 88 centre-de-service@sesam-vitale.fr
Support ASIP Santé	1	Support CPS	CPS Info Service 0 825 85 2000
Support ASIP Santé	1	Support CPS - incident	incident@asipsante.fr
Support ASIP Santé	1	Support CPS - déploiement	jegeneraliselacarte@sante.gouv.fr
Support ASIP Santé Etablissements	2	Support établissements	etablissement@asipsante.fr
Support ASIP Santé DMP-Compatibilité	2	Support DMP	DMPCOMPATIBILITE@sante.gouv.fr
Support ASIP Santé MSSanté	2	Support MSSanté	3657 mssanteinfoservice@sante.gouv.fr
Support ASIP Santé MSSanté	2	Support MSSanté en Etablissement	mssanteinfoservice.es@sante.gouv.fr
Support ASIP Santé MSSanté	2	Support MSSanté aux opérateurs	espacedeconfiance.mssante@sante.gouv.fr
Support ASIP Santé TOM	2	Support TOM	TOM-support-technique@asipsante.fr

Nom	Niveau	Rôle	Contact
Support ASIP Santé RPPS	2	Demande d'extractions RPPS	RPPSextraction@sante.gouv.fr
Support ASIP Santé Annuaire	2	Support Annuaire Santé	annuaire@sante.gouv.fr
Support ASIP Santé Editeurs	3	Support éditeurs, intégrateurs, SIH	editeurs@asipsante.fr
Support ASIP Santé Certificat Classe 4	3	Commande de certificats serveur classe 4	certificat.classe4@asipsante.fr
Support ASIP Santé Certificat Classe 4	3	Commande de certificats et support CleoCPS	support-inscription@asipsante.fr

Tableau 2 : Contacts

4.2 Contacts matériels informatiques et éditions logicielles

Nom	Niveau	Rôle	Contact
Support éditeurs	1, 2 et 3	Support des LPS	Dépendant des éditeurs logiciels
Support Microsoft	1, 2 et 3	Support des PS et SIH sur les produits Microsoft	Dépendant des produits
Support Apple	1, 2 et 3	Support des PS sur les produits Apple	Dépendant des produits
Support Redhat	1, 2 et 3	Support aux intégrateurs et éditeurs sur les produits Redhat	Dépendant des produits
Support lecteurs de cartes à puce	1, 2 et 3	Support aux PS, intégrateurs, éditeurs et SIH sur pour l'intégration et l'utilisation des lecteurs de cartes à puce	Dépendant des fabricants de cartes

Il est indispensable de bien respecter les niveaux de supports en particulier en contactant un support de niveau 1 en premier lieu.

Tableau 3 : Recommandations utilisation niveaux de support

5 Glossaire

Abréviation	Signification
AGPL	Affero General Public License
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
ATS	Answer To Select, réponse de la carte à puce sans contact à la sélection par le lecteur sans contact
ATR	Answer To Reset, réponse de la carte à puce à la mise sous tension
AW PS DMP	Accès Web PS au DMP
CAPI	CryptoAPI, architecture de sécurité Microsoft
CCM	CPS Certificates Manager
CNIL	Commission Nationale de l'Informatique et des Libertés
CDR	Consultation en ligne des droits de l'assuré
CDSA	Common Data Security Architecture, architecture de sécurité Macintosh
CDA	Carte de Directeur de structure Autorisée
CDE	Carte de Directeur d'Établissement
CPA	Carte de Personnel Autorisé
CPE	Carte de Personnel d'Etablissement
CPF	Carte de Professionnel de santé en Formation
CPS	Carte de Professionnel de Santé
CPx	Famille de cartes à puce émises par l'ASIP Santé comprenant CDA, CDE, CPA, CPE, CPF et CPS
CSP	Cryptographic Service Provider, bibliothèque implémentant la Microsoft CryptoAPI (CAPI)

Abréviation	Signification
CVE	Common Vulnerabilities and Exposures
DEB	DEBian software package
DLL	Dynamic Link Library, fichier de bibliothèques logicielles des systèmes d'exploitation Microsoft
DMP	Dossier Médical Personnel
DPKG	Debian PacKaGe management system
EPM	Enhanced Protected Mode – Mode protégé amélioré
ES	Etablissement de Santé
ESR	Extended Support Release
FAQ	Foire Aux Questions
FOT	Facturation en ordre transparent, nouveau projet du GIE SESAM-Vitale permettant la facturation électronique avec des lecteurs PC/SC
FSE	Feuille de Soins Electronique
GALSS	Gestionnaire d'Accès au Lecteur Santé-Social
GPL	General Public License
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS-ECC	Identification Authentification Signature - European Citizen Card
IE	Microsoft Internet Explorer
IGC	Infrastructure de Gestion de Clés, PKI en anglais ou Infrastructure à Clés Publiques i.e. ICP
ISO	International Organization for Standardization
JCA	Java Cryptographic Architecture
JCE	Java Cryptographic Extension
LPS	Logiciel de Professionnel de Santé

Abréviation	Signification
LTS	Long Term Support
MS	Microsoft
MSI	Microsoft Windows Installer, package d'installation Microsoft
MSSanté	Messageries Sécurisées de Santé
OASIS	Organization for the Advancement of Structured Information Standards
ODI	Outil de diagnostic et d'installation
OS	Operating System – Système d'exploitation
OSI	Open Systems Interconnection
OSM	Outils Sécurisés de Messagerie
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure (IGC)
PM	Protected Mode – Mode protégé
PS	Professionnel de Santé
PSS	Protocole Santé social
RDP	Remote Desktop Protocol
RGS	Référentiel Général de Sécurité
RPM	Redhat Package Manager
SI	Système d'Information
SSL	Secure Sockets Layer
TBW	A compléter
TLS	Transport Layer Security
TSE	Terminal Server Edition

Abréviation	Signification
UAC	User Account Control
URL	Uniform Resource Locator
WMI	Windows Management Instrumentation

Tableau 4 : Glossaire

6 Liste des entreprises citées

Le présent document cite les produits des entreprises ou organismes suivants:

Nom	Site Web	Lien avec la Cryptolib CPS
ANSSI	www.ssi.gouv.fr	Co-rédacteur du RGS, Recommandations sans-contact
Apple	www.apple.com	Mac OS X
BouncyCastle	www.bouncycastle.org	API cryptographique pour C# et Java
Citrix	www.citrix.com	Env. TSE/Citrix
Debian	www.debian.org	Linux, .deb
Fedora	fedoraproject.org	Linux, .rpm
Google	www.google.com	Google Chrome
GIE SESAM-Vitale	www.sesam-vitale.fr	PSS, GALSS, API de lecture Vitale
GIXEL	www.gixel.fr	Standard IAS-ECC
HID	www.hidglobal.fr	Fabricant de lecteurs
Idrix	www.idrix.fr	P/Invoke C# CSP
Ingenico	www.ingenico.fr	Fabricant de lecteurs
Microsoft	www.microsoft.com	Windows, CSP, Internet Explorer, C#, .NET, TSE
Mozilla	www.mozilla.org	Mozilla Firefox
Navigo	navigo.fr	Distributeur de lecteur PC/SC compatibles CPx sur Paris/Ile-de-France
NXP Semiconductors	www.nxp.com	Société propriétaire de Mifare, technologie sans-contact souvent mise en relation avec la partie sans contact de la CPS3
OASIS	www.oasis-open.org	Responsable des évolutions du Standard PKCS#11 depuis sa version 2.3
OpenSC	https://github.com/OpenSC/	Outils et librairies pour la carte à puces
Oracle	www.oracle.com	Java, SunMSCAPI
PC/SC Lite	ludovic.rousseau.free.fr	PC/SC sous Linux
PC/SC Workgroup	www.pcscworkgroup.com	Responsable du standard PC/SC visant l'intégration de la carte à puce et des lecteurs de cartes dans les systèmes informatiques
PKCS11Interop	www.pkcs11interop.net	P/Invoke C# PKCS#11
Redhat	www.redhat.com	Linux, .rpm
RSA Security Inc.	www.rsa.com	PKCS, RSA
SpringCard	www.springcard.com	Articles techniques et outils libres relatifs à la carte à puces
Graz University of Technology (Tugraz)	jce.iaik.tugraz.at	Wrapper IAIK PKCS#11 pour Java / JCA

Tableau 5 : Entreprises citées

7 Avertissements

Sur le nécessaire strict respect des procédures décrites dans le manuel L'attention de l'utilisateur est attirée sur l'importance de respecter strictement les procédures décrites dans le présent manuel d'installation et d'utilisation de la Cryptolib CPS v5. Toutes les procédures qui y sont décrites ont été préalablement testées par l'ASIP Santé. Elles doivent permettre à l'utilisateur d'installer et d'utiliser la Cryptolib CPS v5 sur son poste de travail ou tout autre dispositif informatique. En cas de non-respect de ces procédures et des conditions normales d'utilisation de la Cryptolib CPS v5, sa mise en œuvre est susceptible d'engendrer des dysfonctionnements dans l'environnement de travail de l'utilisateur. En cas de dysfonctionnement, quel qu'il soit, l'ASIP Santé prêtera dans la mesure du possible assistance à l'utilisateur, qui ne pourra rechercher sa responsabilité en cas de non-respect des procédures décrites dans le présent manuel.
Sur les liens externes Le présent manuel contient des liens vers des sites Internet. Ces liens ne visent qu'à informer l'utilisateur. Ces sites Web ne sont pas gérés par l'ASIP Santé et l'ASIP Santé n'exerce sur eux aucun contrôle : leur mention ne saurait engager l'ASIP Santé quant à leur contenu. L'utilisation des sites tiers mentionnés relève de la seule responsabilité du lecteur ou de l'utilisateur des produits documentés.
Sur les copies d'écran et les lignes de commande Les lignes de commandes données ci-après le sont à titre indicatif. Elles documentent des cas « passants » qui peuvent différer d'un système à l'autre. Les copies d'écran présentées dans ce document sont données à titre illustratif. Les pages ou écrans réellement affichés peuvent être différents, notamment en raison de montées de version ou de configurations d'environnements différentes.
Citations L'ASIP Santé est contrainte de citer le nom de certaines entreprises recensées au tableau n°5 afin d'apporter toute l'aide nécessaire aux utilisateurs de la Cryptolib CPS v5 dans son installation et son utilisation. Les entreprises citées peuvent prendre contact avec l'ASIP Santé à l'adresse email editeurs@asipsante.fr pour toute demande en lien avec la citation les concernant. Les entreprises non citées dans ce manuel et ayant une activité en lien avec la Cryptolib CPS v5 peuvent également se faire connaître auprès de l'ASIP Santé en la contactant à la même adresse.
Contact Toute question en rapport avec le contenu du présent manuel doit être adressée à l'adresse suivante: editeurs@asipsante.fr

Tableau 6 : Avertissements

8 Présentation générale

8.1 La famille de cartes CPx

Les cartes CPx permettent d'effectuer des opérations cryptographiques dont l'objectif est de sécuriser des actions ou des échanges informatiques.

Les cartes CPx sont exhaustivement présentées en **[5]** et permettent de mettre en œuvre le palier 3 de l'authentification publique des acteurs de Santé comme décrit en **[20]**. La carte CPx constitue non seulement la carte d'identité du PS mais elle atteste aussi d'un processus d'enrôlement natif à l'espace de confiance ADELI/RPPS. A ce titre, la carte CPx est éligible à l'authentification publique.

En résumé, les cartes CPx offrent deux grandes fonctions:

1. L'authentification, privée et publique
    a. qui permet d'authentifier de manière forte le porteur de la carte CPx
2. La signature numérique
    a. qui permet de vérifier l'authenticité et l'intégrité d'un document lors de sa réception

L'exploitation de la carte CPx sur un poste de travail passe par l'installation:

- D'un lecteur de carte connecté physiquement sur le poste de travail
    - dans lequel sera introduite la carte CPx
- de la Cryptolib CPS

A partir de la CPx v3, toutes les cartes CPx présentent un volet sans-contact décrit en **[27].**

8.2 La Cryptolib CPS: bibliothèque cryptographique des cartes CPx

Les systèmes d'exploitation modernes prévoient tous la possibilité d'installer et de faire fonctionner un lecteur et une carte à puce. Pour répondre à la diversité des matériels, les éditeurs des systèmes d'exploitation documentent des « API » qui servent de points d'ancrage aux fabricants de lecteurs ou de cartes dans les systèmes cibles.

Quels que soient le lecteur de cartes ou la carte à puce utilisés, il est donc nécessaire d'installer des composants logiciels additionnels:

1. Un « Pilote » (« driver ») pour le lecteur
    a. afin de « gommer » les spécificités du lecteur auprès de l'OS
2. Des logiciels d'accès à la carte à puce (« middleware »)
    a. afin de « gommer » les spécificités cryptographiques de la carte à puce vis-à-vis des logiciels qui l'exploitent

Une fois ces deux composants additionnels correctement installés sur le poste de travail, les logiciels traditionnels tels que les navigateurs Internet ou les outils de messageries peuvent exploiter les fonctionnalités offertes par la carte à puce indépendamment de son type et du lecteur de carte dans lequel elle est insérée.

La Cryptolib CPS implémente ces points d'ancrage pour les cartes CPx et pour les systèmes Windows, Mac OS X et Linux.

8.3 Le cycle de vie de la Cryptolib CPS sur le poste de travail

Le cycle de vie de la Cryptolib CPS sur un poste de travail, quel que soit le système d'exploitation, est le suivant :

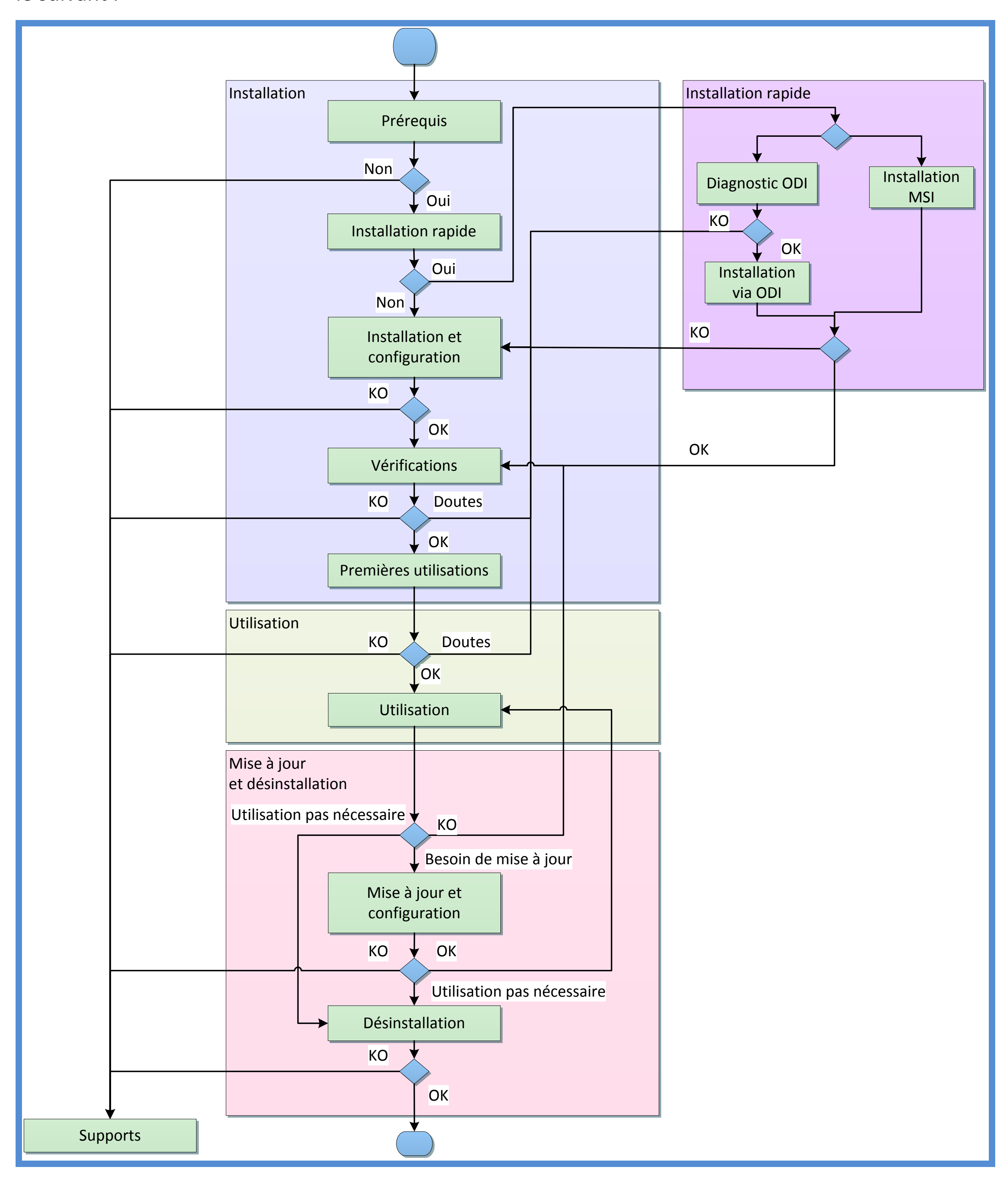


Figure 1 : Cryptolib CPS : cycle de vie sur le poste de travail.

Ce cycle de vie est détaillé dans la suite du document.

9 Prérequis

Ce document ne couvre pas la partie « Pilote de lecteur de cartes ». Il est nécessaire de se reporter aux modes d'emploi des matériels mis en œuvre par ailleurs.

Ce document couvre la partie « installation et utilisation de la Cryptolib CPS » qui fait office de « middleware » pour les cartes CPx distribuées par l'ASIP Santé.

9.1 Prérequis matériels

Prérequis matériels pour l'installation et l'utilisation de la Cryptolib CPS

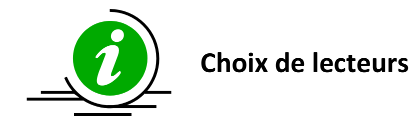
	#	Description	Précisions
Matériels	**1**	Ordinateurs PC ou MAC équipés de processeurs Intel ou AMD, architecture x86 ou x64	Ces matériels concernent généralement les Personnels de santé libéraux ou les petites structures
	2	Serveurs équipés de processeurs Intel ou AMD, architecture x86 ou x64. Les architectures IA64 ne sont pas supportées.	Ces matériels concernent généralement les structures mettant en œuvre des machines en réseau, ou des hébergeurs de services
	3	Les processeurs PowerPC ne sont plus supportés	Mac OS X 10.5 est la dernière version de Mac OS X à supporter PowerPC
	4	Lecteurs de cartes à puce avec firmwares à jour correctement installés et configurés • PSS bi-fente de type FSE • ou PSS mono-fente NF-CPS • ou mono-fente PC/SC	cf. manuels et fournitures du fabriquant du matériel concerné. Pour les lecteurs PC/SC : • Les lecteurs Navigo sont compatibles. • Vérifier l'existence d'outils de diagnostic lecteur. • Préférer les lecteurs USB compatibles CCID[6]. Pour les lecteurs PSS : • Préférer les lecteurs supportés par le GIE-SV[7]
	5	Une carte CPS2Ter ou CPS3 • dont le code porteur est connu et non bloqué • non expirée • non révoquée	Les cartes CPS2Ter arrivent en fin de vie en avril 2014

[6] La liste pour Apple Mac OS 10.09 et Debian. La liste pour Apple Mac OX 10.10. Pour Microsoft Windows, le programme « Windows hardware certification » assure que les lecteurs sont compatibles avec le driver USB CCID usbccid.sys présent par défaut dans les OS Microsoft.

[7] La liste pour les PS libéraux, la liste pour les établissements

Prérequis matériels pour l'installation et l'utilisation de la Cryptolib CPS			
	#	**Description**	**Précisions**
	6	La Cryptolib CPS occupe environ 50MB et ne nécessite que très peu de ressources systèmes pour fonctionner.	Cf. Recommandations de l'éditeur du système d'exploitation pour la RAM, la fréquence CPU et la taille du disque dur nécessaires.
L'ASIP Santé et le GIE SESAM-Vitale émettent des recommandations matérielles communes pour les lecteurs PC/SC au travers de **[7]**. L'ASIP Santé n'émet aucune recommandation particulière relative aux marques des matériels. Ce guide contient des recommandations supplémentaires concernant les lecteurs dans la partie « sans contact » (carte CPS3 et Cryptolib CPS v5).			

Tableau 7 : Prérequis : Matériels



	Choix de lecteurs	La question du choix de lecteur est abordée exhaustivement en annexe.

Tableau 8 : Prérequis : Matériels : Choix de lecteur

9.2 Prérequis sur les systèmes d'exploitation

Prérequis sur les systèmes d'exploitation pour l'installation et l'utilisation de la Cryptolib CPS				
	#	**OS**	**Version**	**Fin de support éditeur**
Système d'exploitation	**1**	Windows	Windows XP SP3 (32bit)[8]	avril 2014
	2		Windows 7 SP1 (32 et 64 bits)	janvier 2020
	3		Windows 8.1 (32 et 64 bits)	janvier 2023
	4		Windows 2003 Server R2 SP2 (32 et 64 bits)	juillet 2015
	5		Windows 2008 Server R2 SP2 (64 bits)	janvier 2020
	6	Mac OS X	Apple Mac OS X 10.7[9]	N/A
	7		Apple Mac OS X 10.8	
	8		Apple Mac OS X 10.9	
	9	Linux	Fedora 19 (RPM)	Préférer les versions « LTS »
			Redhat (RPM)	
			Mint Linux (DEB)	Préférer les versions « LTS » Consulter l'ASIP Santé
			Mageia (ex. Mandriva Linux) (RPM)	
			Ubuntu (DEB)	
			openSUSE (RPM)	
			Debian (DEB)	
L'ASIP Santé n'émet aucune recommandation particulière concernant les systèmes d'exploitation.				

Tableau 9 : Prérequis : Système d'exploitation

[8] Suite à la fin de support de Windows XP par Microsoft intervenue le 08/04/2014, l'ASIP Santé continue d'assurer le support technique jusqu'au 15 avril 2015 sur les livrables diffusés jusqu'au 08 avril 2014. Cf. http://integrateurs-cps.asipsante.fr/informations_cps/Fin-du-support-Windows-XP pour plus d'information.

[9] Apple Mac OS X 10.6 n'est plus supporté par l'ASIP Santé depuis le premier semestre 2014.

9.3 Prérequis logiciels

Prérequis logiciels pour l'installation et l'utilisation de la Cryptolib CPS			
	#	**Description**	**Précisions**
Logiciels	**1**	Navigateurs : • Microsoft Internet Explorer • Google Chrome • Mozilla Firefox • Safari	Nécessaires pour une installation via ODI
	2	Oracle Java Virtual Machine (JVM) 1.6+	Nécessaires pour une installation via ODI. Attention aux actions de mise à jour de la JVM (impact sur les logiciels utilisant Java, impact sur les logiciels utilisant des applets Java).
	3	Plugin Java pour les navigateurs web et JavaScript activés	Nécessaires pour une installation via ODI
	4	Adobe Acrobat Reader	Facultatif sur les machines de production. Requis afin de consulter la documentation.
	5	Sous Windows: • Les fichiers de type MSI doivent pouvoir être installés • L'UAC peut être activée	Sous Windows: • Les droits administrateurs ne sont pas requis en première intention (voir plus loin) • Les droits des comptes par défaut sont suffisants
	6	Les installations sont généralement possibles avec des antivirus activés.	L'ASIP Santé ne teste pas de configuration avec antivirus. Attention aux actions de désactivation de l'antivirus. Attention aux « sandbox » lors des vérifications fonctionnelles. Cf. manuel des éditeurs d'antivirus Certains antivirus ou anti-malware désactive le module XPI d'extension Firefox de l'ASIP Sante (module de sécurité CPS)

<table>
<tr><td colspan="7">Prérequis logiciels pour l'installation et l'utilisation de la Cryptolib CPS</td></tr>
<tr><th></th><th>#</th><th colspan="4">Description</th><th>Précisions</th></tr>
<tr><td rowspan="9"></td><td>7</td><td colspan="4">Les installations sont généralement possibles sur des postes protégés par un firewall.</td><td>ODI télécharge en particulier des fichiers de type:
• .jar
• .jnlp
• .zip
• .msi</td></tr>
<tr><td>8</td><td colspan="4">GALSS, distribué par le GIE SESAM-Vitale, pour les lecteurs PSS</td><td>La dernière version est préconisée.</td></tr>
<tr><td rowspan="7">9</td><td rowspan="7">Services</td><td rowspan="3">Windows</td><td>ScardSvr</td><td>carte à puce</td><td rowspan="7">Les services de gestion de cartes à puces doivent être présents.

Sous Windows, le .MSI lance le service SCardSvr.

Sous Linux, le .RPM assure le démarrage de pcscd au boot.</td></tr>
<tr><td>Msiserver</td><td>MSI</td></tr>
<tr><td>CertPropSvc</td><td>propagation</td></tr>
<tr><td>Mac OS X</td><td colspan="2">pcscd</td></tr>
<tr><td rowspan="2">Linux</td><td>PC/SC</td><td>pcscd
libpcsclite-dev</td></tr>
<tr><td>PSS</td><td>usbserial</td></tr>
<tr></tr>
<tr><td colspan="7">L'ASIP Santé n'émet aucune recommandation logicielle particulière.</td></tr>
</table>

Tableau 10 : Prérequis : Logiciels

9.4 Prérequis sur l'accès Internet

<table>
<tr><td colspan="4">Prérequis sur l'accès Internet pour l'installation et l'utilisation de la Cryptolib CPS</td></tr>
<tr><th></th><th>#</th><th>Site</th><th>Description</th></tr>
<tr><td rowspan="5">Accès Internet</td><td>1</td><td>Accès à http://integrateurs-cps.asipsante.fr/</td><td>Facultatif.
Généralement réservé aux éditeurs et aux établissements.
Nécessaire si le GALSS n'est pas fournie avec un logiciel « tiers ».
Accès protégé par mot de passe.</td></tr>
<tr><td>2</td><td>Accès à http://testssl.asipsante.fr
et à https://testssl.asipsante.fr</td><td>Facultatif pour l'installation.

Très utile pour la vérification de l'installation.</td></tr>
<tr><td>3</td><td>Accès à
http://annuaire.asipsante.fr
http://annuaire.gip-cps.fr</td><td>Facultatif pour l'installation.

Nécessaire pour des cas d'usage avancés (signatures et vérifications de signatures avec Outlook par exemple)</td></tr>
<tr><td>4</td><td>Accès à http://www.outil-diagnostic.asipsante.fr/</td><td>Nécessaire pour une installation par ODI.</td></tr>
<tr><td>5</td><td>Accès à http://esante.gouv.fr/</td><td>Nécessaire
• Accès aux documents ASIP Santé.
• Accès libre aux installeurs de la Cryptolib CPS.</td></tr>
<tr><td colspan="4">L'ASIP Santé n'émet aucune recommandation sur le fournisseur d'accès à Internet.</td></tr>
</table>

Tableau 11 : Prérequis : Connexion d'accès à Internet

9.5 Prérequis sur les versions de la Cryptolib CPS

Prérequis sur les versions de la Cryptolib CPS

	#	Version	Spécificités
Cryptolib CPS	1	Cryptolib CPS v4 « filière GALSS »	adresse les cartes CPS2Ter et les cartes CPS3
			exploite le profil CPS2Ter uniquement sur les cartes CPS3
			fonctionne avec le GALSS et les lecteurs PSS ou PC/SC
			cette documentation adresse expressément cette filière
			ne pas l'installer en parallèle de la « Cryptolib CPS v4 Full PC/SC »
	2	Cryptolib CPS v4 « filière PC/SC »	adresse les cartes CPS2Ter et les cartes CPS3
			exploite le profil CPS2Ter uniquement sur les cartes CPS3
			fonctionne avec les lecteurs PC/SC uniquement
			bien que cette documentation n'adresse pas expressément cette filière, l'essentiel de l'information qu'elle contient est valable pour la filière Full PC/SC modulo le fait de ne pas installer préalablement le GALSS
			l'installation de cette filière est vivement recommandée : • **Pour les postes équipés uniquement de lecteurs PC/SC** • **En particulier pour les postes de développements**
			l'installation de cette filière était obligatoire pour faire du Smartcard logon avec la Cryptolib CPS v4. **Le Smartcard logon est désormais supporté avec la Cryptolib CPS v5 uniquement et fait l'objet d'un document dédié [17].**
			préférer l'utilisation de la Cryptolib CPS v5 qui factorise les 2 filières
			ne pas l'installer en parallèle de la « Cryptolib CPS v4 GALSS »

Prérequis sur les versions de la Cryptolib CPS			
	#	**Version**	**Spécificités**
	3	Cryptolib CPS v5	**factorise** les filières GALSS et PC/SC
			adresse les cartes CPS2Ter et les cartes **CPS3**
			exploite le **profil CPS3** (IAS-ECC) sur les cartes CPS3
			n'exploite **pas** le profil CPS2Ter sur les cartes CPS3
			exploite le **profil sans contact** de la carte **CPS3** (pas de sans contact en CPS2ter)
			installe la Cryptolib CPS v4 en parallèle (cf. ci-après)
			est disponible en **32b et 64b** sous Windows
Consulter le support de l'éditeur du LPS pour vérifier la compatibilité de la version du LPS avec la version de la Cryptolib CPS visée.			

Tableau 12 : Prérequis : Versions des Cryptolib CPS

La Cryptolib CPS **v3** n'est plus supportée. Les remarques liées à son installation sont néanmoins conservées, pour mémoire ou pour comparaison avec les versions Cryptolib CPS **v4** et Cryptolib CPS **v5.**

Tout au long de ce document, les labels « **v3** », « **v4** », « **v4 Full PC/SC** » et « **v5** » rappellent la version de Cryptolib CPS à laquelle se réfère la remarque/mention/précision courante.

9.6 Téléchargements logiciels

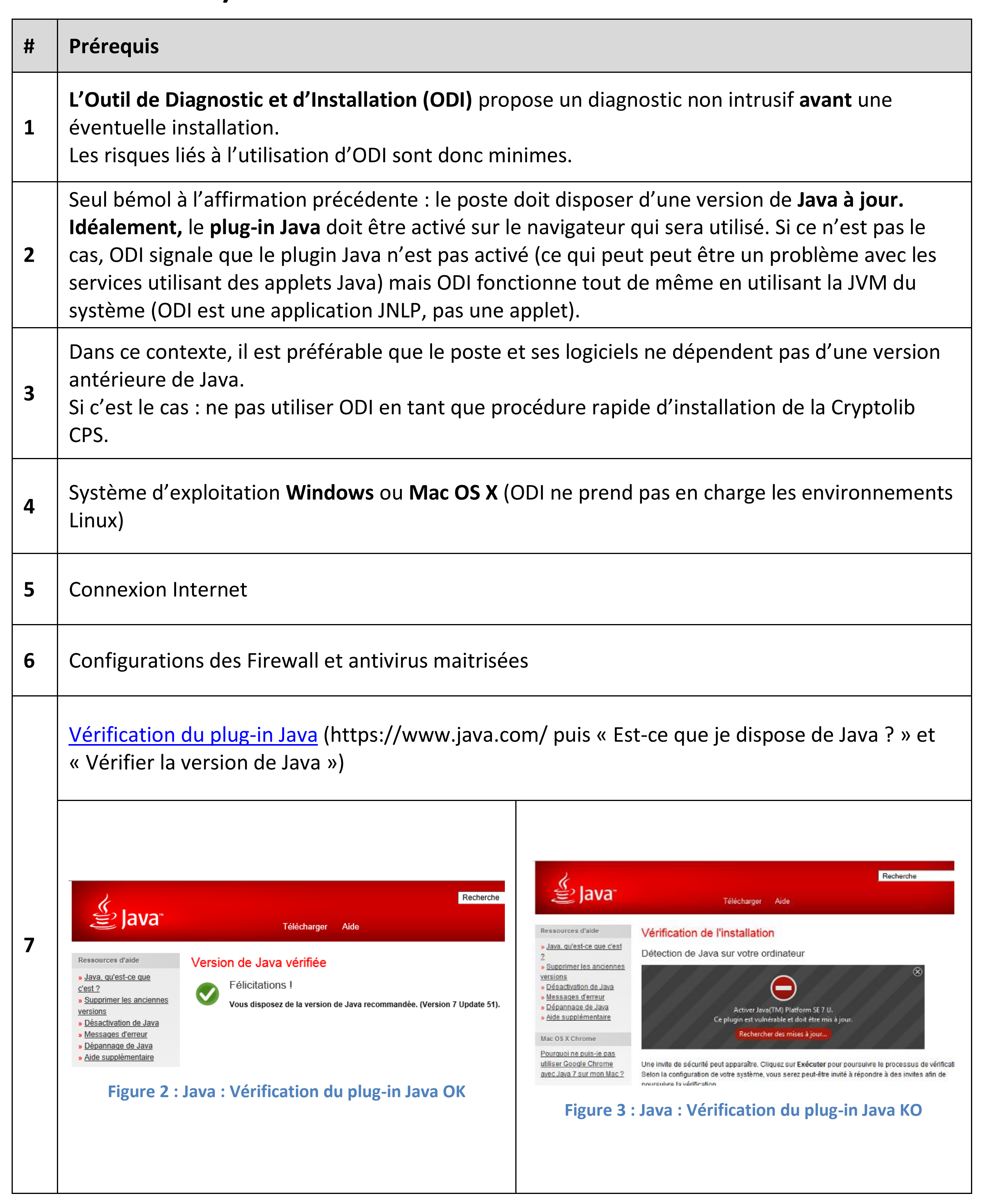
Les composants logiciels sont téléchargeables au choix depuis :

#	**Téléchargements logiciels**	
1	Cryptolib CPS	Espace Téléchargements logiciels esante.gouv.fr **[19]**
2	Cryptolib CPS	Espace intégrateurs ASIP Santé
3	GALSS	Espace intégrateurs ASIP Santé
4	Cryptolib CPS / GALSS	Installeurs logiciels LPS

Tableau 13 : Installation: Sources des installeurs

10Procédures rapides d'installation du poste de travail

10.1 Installation du poste de travail via ODI (OS Windows et Mac OS X)



#	Prérequis
1	**L'Outil de Diagnostic et d'Installation (ODI)** propose un diagnostic non intrusif **avant** une éventuelle installation. Les risques liés à l'utilisation d'ODI sont donc minimes.
2	Seul bémol à l'affirmation précédente : le poste doit disposer d'une version de **Java à jour. Idéalement,** le **plug-in Java** doit être activé sur le navigateur qui sera utilisé. Si ce n'est pas le cas, ODI signale que le plugin Java n'est pas activé (ce qui peut peut être un problème avec les services utilisant des applets Java) mais ODI fonctionne tout de même en utilisant la JVM du système (ODI est une application JNLP, pas une applet).
3	Dans ce contexte, il est préférable que le poste et ses logiciels ne dépendent pas d'une version antérieure de Java. Si c'est le cas : ne pas utiliser ODI en tant que procédure rapide d'installation de la Cryptolib CPS.
4	Système d'exploitation **Windows** ou **Mac OS X** (ODI ne prend pas en charge les environnements Linux)
5	Connexion Internet
6	Configurations des Firewall et antivirus maitrisées
7	Vérification du plug-in Java (https://www.java.com/ puis « Est-ce que je dispose de Java ? » et « Vérifier la version de Java ») Figure 2 : Java : Vérification du plug-in Java OK Figure 3 : Java : Vérification du plug-in Java KO

#	Prérequis
8	N'avoir besoin que de la Cryptolib CPS v4 GALSS et du GALSS (ODI n'installe pas encore la Cryptolib CPS v5).
9	Disposer d'un ordinateur Windows ou Mac OS X déjà équipé physiquement d'un lecteur • PSS bi-fente de type FSE • ou PSS mono-fente NF-CPS • ou mono-fente PC/SC
10	Disposer d'une carte CPx • non bloquée • dont le code porteur est connu • non expirée • non révoquée

Tableau 14 : Installation rapide : ODI : Prérequis

#	**Installation**
1	Arrêter toutes les applications, en particulier les applications et toutes les sessions utilisant ces applications qui accèdent à la carte CPx.
2	Se rendre sur le portail ODI **[2]**
3	Choisir la version de l'installeur en fonction de l'application ciblée • toutes les versions d'ODI installent la Cryptolib CPS • seuls les messages de diagnostic peuvent différer (liés aux contraintes imposées par chaque application)
4	Lire le manuel ODI de la version choisie
5	Lancer le diagnostic
6	En fonction du diagnostic, une mise à jour logicielle peut être proposée par ODI • enregistrer une copie du Rapport technique avant de lancer la mise à jour • lancer les installations en cliquant sur le bouton « MISE A JOUR LOGICIELLE »

Tableau 15 : Installation rapide : ODI : Installation

#	**Vérifications**
1	CPS-Gestion affiche les données d'identification du porteur et de la carte
2	CCM passe au vert
3	Les magasins de certificats sont provisionnés
4	Le test d'authentification SSL avec un navigateur et http://testssl.asipsante.fr est OK

Tableau 16 : Installation rapide : ODI : Vérifications

#	Les limitations d'ODI
1	ODI fonctionne avec les versions 1.7.0_51 (01/2014) et 1.7.0_45 (10/2013) de Java.
2	Avec ODI v5, le navigateur, le plugin Java et le JRE installés sur le poste peuvent être 32bits ou 64bits.
3	ODI v5 installe la Cryptolib CPS v5 32bits. ODI v5 n'installe le GALSS que si un lecteur PSS est préalablement branché au poste de travail.
4	Sous Mozilla Firefox, l'utilisateur doit prêter attention au mécanisme de « Click-to-play » pour activer le plug-in Java. Figure 4 : Mozilla Firefox : Click-to-play
5	Depuis le 09/09/2014, Microsoft internet Explorer **bloque** les versions obsolètes du plug-in Java. L'utilisateur doit donc prêter attention aux messages que le navigateur lui affiche (référence : http://blogs.msdn.com/b/ie/archive/2014/08/06/internet-explorer-begins-blocking-out-of-date-activex-controls.aspx et https://technet.microsoft.com/library/security/ms14-sep)
6	A partir de Chrome 42, les plugins NPAPI sont bloqués par défaut (https://www.chromium.org/developers/npapi-deprecation): • passer par les « flags » : o chrome://flags/#enable-npapi • passer par la ligne de commande : o --enable-npapi o --always-authorize-plugins • passer par la base de registre : o Software\Policies\Chromium\EnabledPlugins o Software\Policies\Google\Chrome\PluginsAllowedForUrls • passer par les GPO (Chrome Policy Templates): o EnabledPlugins_Policy="Indiquer une liste de plug-ins activés" (Google Chrome) o PluginsAllowedForUrls_Policy="Autoriser les plug-ins sur ces sites" (Google Chrome > Paramètres de contenu)
7	ODI utilise le cache Java, qui doit être activé et éventuellement purgé en cas d'instabilités avérées (cf. Gestion cache Java).

#	Les limitations d'ODI
8	Des problèmes de figeage d'ODI ont pu être constatés avec l'antivirus Avast, qui peut être désactivé jusqu'au prochain redémarrage, le temps de l'installation ODI, sous réserve de prendre toutes les précautions de sécurité en parallèle (pas d'installation de logiciels tiers ou de navigation web en parallèle par exemple).
9	Avec ODI v5, l'outil fonctionne avec des connexions HTTP/HTTPS configurées pour utiliser un proxy.
10	ODI n'est pas destiné aux déploiements sur des réseaux administrés (typiquement en établissement de santé). Préférer l'utilisation du Pack Etablissement (cf. site integrateurs-cps.asipsante.fr) dans ces cas de figure.

Tableau 17 : Installation rapide : ODI : Limitations

10.2 Installation du poste de travail via les MSI sous Windows

#	Prérequis
1	Avoir peu de doute sur les prérequis listés plus haut
2	Connaissances en informatique
3	Connexion internet
3	Disposer d'un ordinateur Windows, Mac OS X ou Linux déjà équipé physiquement d'un lecteur • PSS bi-fente de type FSE • ou PSS mono-fente NF-CPS • ou mono-fente PC/SC
4	Disposer d'une carte CPx • non bloquée • code porteur connu • non expirée • non révoquée

Tableau 18 : Installation rapide : MSI sous Windows : Prérequis

#	Installation
1	Arrêter toutes les applications, en particulier celles qui accèdent à la carte CPS.
2	Télécharger les derniers composants logiciels
3	Exécuter l'installation à partir du package logiciel récupéré • installer le GALSS « **galss-x.yy.zz.msi »** Puis • installer la Cryptolib CPS « **CryptolibCPS-x.y.z.msi** »
4	Relancer la machine si demandé

Tableau 19 : Installation rapide : MSI sous Windows : Installation

#	Vérifications
1	CPS-Gestion affiche les données d'identification du porteur et de la carte
2	CCM passe au vert
3	Les magasins de certificats sont provisionnés
4	Le test d'authentification SSL avec un navigateur et http://testssl.asipsante.fr est OK

Tableau 20 : Installation rapide : MSI sous Windows : Vérifications

11Installation de la Cryptolib CPS

11.1 Préparation de l'installation

#	Préparation de l'installation
1	**Vérifier les prérequis**
	Prérequis matériels Prérequis sur les systèmes d'exploitation Prérequis logiciels Prérequis sur l'accès Internet Prérequis sur les versions de la Cryptolib CPS
2	**Le système d'exploitation (OS) de la machine doit être l'un des trois :**
	Windows (Windows XP SP3, Server 2003, Server 2008, Windows 7 SP1, Windows 8.1) Mac OS X (à partir de la version 10.6)[10] Linux (Noyau 2.4 ou 2.6)
3	**Au moins un des trois types de lecteurs suivants est connecté à la machine:**
	Lecteur bi-fente « SESAM-Vitale » connecté sur un port COM.
	La valeur constructeur par défaut de l'adresse physique (« PAD ») de ce type de lecteur est configurée à 2 L'installeur du GALSS met la valeur du « PAD » à 2 dans le fichier galss.ini Cette valeur peut être changée par manipulation sur le lecteur auquel cas cette valeur doit être reportée en cohérence dans le galss.ini cf. la documentation du lecteur pour la configuration de ce paramètre
	Lecteur mono-fente « NF CPS » connecté sur un port COM.
	La valeur constructeur par défaut de l'adresse physique (« PAD ») de ce type de lecteur est configurée à 0 L'installeur du GALSS met la valeur du « PAD » à 0 dans le fichier galss.ini Cette valeur peut être changée par manipulation sur le lecteur auquel cas cette valeur doit être reportée en cohérence dans le galss.ini cf. la documentation du lecteur pour la configuration de ce paramètre
	Lecteur mono-fente « PC/SC » quel que soit son type de connexion
	Il faut que le lecteur soit physiquement connecté à la machine et que son pilote (« driver ») PC/SC ait été préalablement installé avec succès (driver à rechercher auprès du fournisseur).
4	**Il est également conseillé d'avoir effectué un arrêt et un redémarrage de la machine pour une bonne prise en compte du lecteur PC/SC**
5	**La carte CPx est insérée dans le lecteur**
6	**Un éventuel redémarrage de la machine est anticipé:**
	Tous les documents, fichiers ou applications « sensibles » sont fermés Toutes les applications ou utilitaires accédant à la CPS sont fermés Les navigateurs et outils de messagerie sont fermés

Tableau 21 : Préparation de l'installation

[10] La prise en charge des lecteurs série (i.e. lecteurs bi-fente) avec le navigateur Safari sous Léopard (OS X 10.5) n'est possible qu'à partir de la release 10.5.6 de cet OS. Cet OS n'est aujourd'hui plus supporté.

11.2 Logique d'installation

Une fois les prérequis vérifiés, la logique d'installation est la suivante :

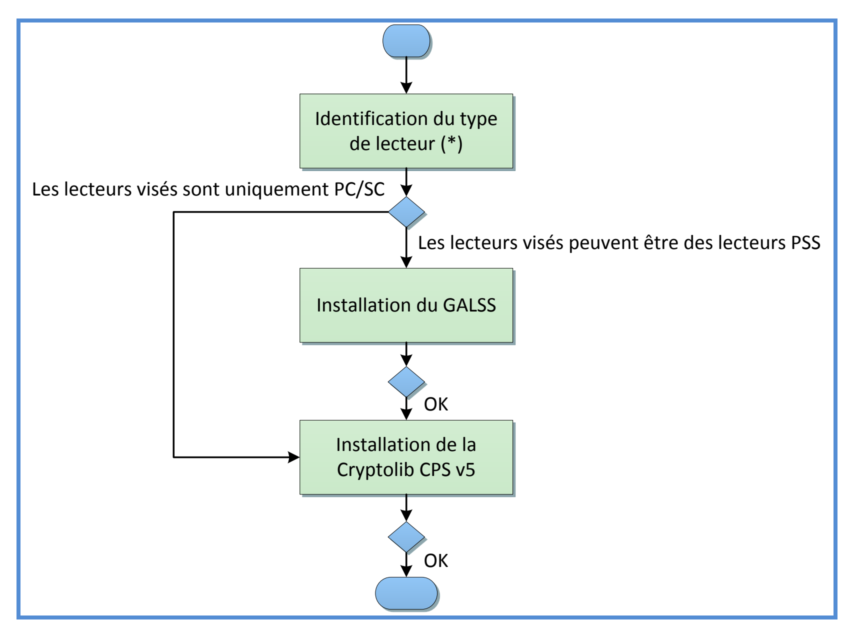


Figure 5 : Cryptolib CPS : logique d'installation

#	Remarques concernant la logique d'installation
*	Pour des indications sur l'identification du type de lecteur visé, voir « Annexe – Choix de lecteur »
1	Depuis la **Cryptolib CPS v4**, la Cryptolib CPS n'installe plus le **GALSS**. L'installation correcte des pilotes des lecteurs de carte est un prérequis important à l'installation de la **Cryptolib CPS**. Le **GALSS** est considéré, vu de la **Cryptolib CPS**, **comme** le **pilote** des **lecteurs** PSS.
2	L'ordre d'installation **Cryptolib CPS / GALSS** n'a pas d'importance.
3	En fusionnant les filières GALSS et Full PC/SC, la **Cryptolib CPS v5** assouplit les conditions de migrations « lecteurs PSS » vers « lecteurs PC/SC ».
4	La **Cryptolib CPS v4 GALSS** n'est plus supportée. Préférer l'installation de la **Cryptolib CPS v5**.
5	La **Cryptolib CPS v4 Full PC/SC** n'est plus supportée. Préférer l'installation de la **Cryptolib CPS v5**.
En cas de doute, contacter les supports • logiciels LPS • ASIP Santé pour confirmer la pertinence de l'installation de la Cryptolib CPS v4 (Full PC/SC ou GALSS)	

Tableau 22 : Cryptolib CPS: Remarques sur la procédure d'installation

11.3 Installation du GALSS

Cette procédure ne s'applique pas avec la Cryptolib CPS v4 Full PC/SC

#	GALSS : Remarques préalables à la procédure d'installation du GALSS
1	Les versions 4 ou supérieures de la Cryptolib CPS n'installent pas le GALSS.
2	L'utilisation de la dernière version du GALSS est recommandée.
3	L'installeur du GALSS détecte les lecteurs de carte physiquement connecté à la machine et crée un fichier « galss.ini » en conséquence. **Il est donc essentiel de connecter le lecteur de carte au poste de travail avant de lancer l'installation du GALSS.**
4	Le composant GALSS n'est pas en lui-même compliqué à installer. Par contre, il est utilisé par de nombreux logiciels présents sur les postes. Son installation ou sa mise à jour peuvent être très impactantes pour le fonctionnement du poste (perte complète des fonctionnalités possible). La préparation de l'installation doit donc être minutieuse. Les logiciels LPS présents sur le poste et utilisant le GALSS doivent avoir été qualifiés pour la version de GALSS qui va être installée. En cas de doute, il est préférable de contacter le support de l'éditeur logiciel afin d'obtenir la confirmation de la compatibilité entre la version courante du LPS et la version du GALSS à installer.
5	Les informations contenues dans le fichier **galss.ini** sont essentielles. Si les informations contenues dans le fichier **galss.ini** s'avéraient être décorrélées par rapport aux connexions physiques {lecteurs, poste de travail}, le poste de travail ne pourrait pas mettre en œuvre correctement les cartes CPx insérées dans les lecteurs PSS.
6	Cette documentation n'est pas le guide d'installation et d'utilisation du GALSS. Pour plus de précision, se reporter à **[6]** « GALSS 3.xx - Gestionnaire d'Accès aux Lecteurs Santé Social ».

Tableau 23 : GALSS : Remarques sur la procédure d'installation

La procédure d'installation du GALSS est la suivante :

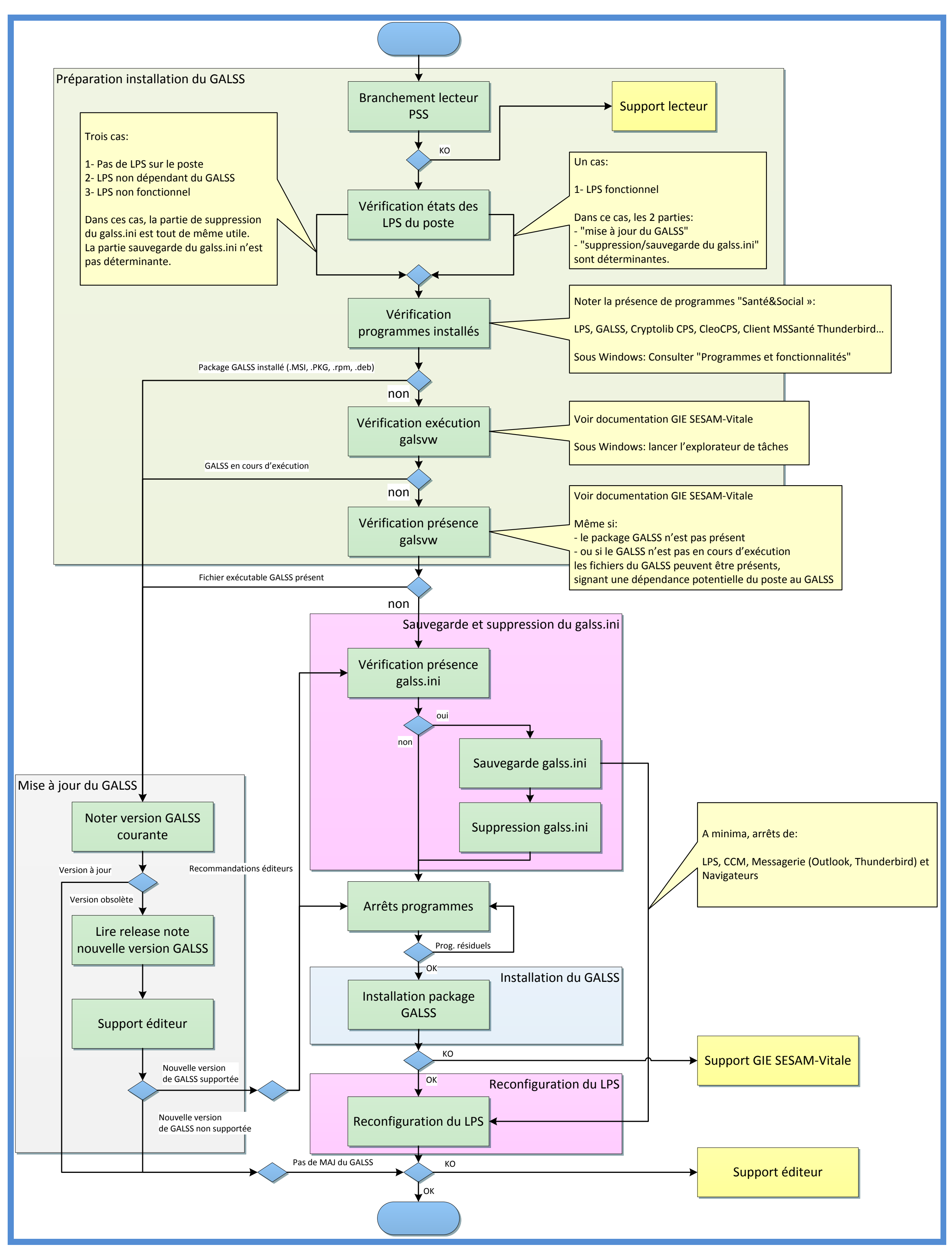


Figure 6 : GALSS : Procédure d'installation

Le composant GALSS ainsi que les logiciels traditionnellement présents sur un poste de travail Santé Social sont sensibles à la qualité du fichier de configuration galss.ini.
Avant d'installer ou de mettre à jour le GALSS, il est donc préférable de sauvegarder toutes les occurrences du fichier galss.ini présentes sur le poste de travail.

<table>
<tr><th>OS</th><th>#</th><th colspan="4">GALSS : Procédure de sauvegarde du fichier galss.ini</th></tr>
<tr><td rowspan="17">Windows</td><td rowspan="4">1</td><td colspan="4"><u>Créer</u> un répertoire de sauvegarde dédié :</td></tr>
<tr><td colspan="2">C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\</td><td colspan="2">Ex. : C:\INSTALLS\GALSS\Config\20120229-01\</td></tr>
<tr><td>yyyyMMdd</td><td>date du jour au format année-mois-jour</td><td>Ex. : 20120229</td><td>date du jour au format année-mois-jour</td></tr>
<tr><td>xx</td><td>numéro de la sauvegarde du jour</td><td>Ex. : 01</td><td>1ere sauvegarde</td></tr>
<tr><td rowspan="9">2</td><td colspan="4"><u>Sauvegarder</u> manuellement les fichiers suivants :</td></tr>
<tr><td colspan="2">Source</td><td>Signalé par ODI</td><td>Destination</td></tr>
<tr><td colspan="2">%WINDIR%\galss.ini</td><td>Oui</td><td>C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\windir\</td></tr>
<tr><td colspan="2">%USERPROFILE%\Windows\galss.ini</td><td>Oui</td><td>C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\userprofile\</td></tr>
<tr><td colspan="2">%USERPROFILE%\AppData\Local\VirtualStore\Windows\galss.ini</td><td>Oui</td><td>C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\virtualstore\</td></tr>
<tr><td colspan="2">%ALLUSERSPROFILE%\santesocial\galss\galss.ini</td><td>Oui</td><td>C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\programdata\</td></tr>
<tr><td colspan="2">%PUBLIC%\AppData\santesocial\galss\galss.ini</td><td>Non</td><td>C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\public\</td></tr>
<tr><td colspan="2">%USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Virtualized\C\ProgramData\santesocial\galss\galss.ini</td><td>Non</td><td>C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\tempinet\</td></tr>
<tr><td colspan="2">%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\VIRTUALIZED\C\PROGRAMDATA\SANTESOCIAL\GALSS\GALSS.INI</td><td>Non</td><td>C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\inetcache\</td></tr>
<tr><td rowspan="2">3</td><td colspan="4"><u>Optionnel</u>: Supprimer manuellement les fichiers galss.ini</td></tr>
<tr><td colspan="2">Même liste d'emplacement que ci-dessus.
La restauration sera possible à partir des fichiers du répertoire C:\INSTALLS\GALSS\Config\yyyyMMdd-xx\</td><td colspan="2">La suppression des fichiers galss.ini est préconisée en cas de :
Réinstallation
Régénération de configuration</td></tr>
</table>

Tableau 24 : GALSS : Procédure de sauvegarde du fichier galss.ini

Sur un poste vierge, la procédure d'installation du GALSS se réduit alors à ceci :

#	GALSS : Procédure d'installation
1	**Connecter le/les lecteur(s) de cartes au poste de poste de travail**
2	**Même si le poste est supposé être vierge: appliquer la procédure « GALSS : Procédure de régénération du fichier galss.ini » décrite ci-dessus**
3	Télécharger les derniers composants logiciels, dont le GALSS
4	Installer le GALSS • Se reporter à la documentation du GIE SESAM-Vitale ○ Cf. **[6]** • L'installeur GALSS prend la forme ○ Sous Windows : d'un fichier .MSI ○ Sous Mac OS X : d'un fichier .PKG embarqué dans un .DMG ○ Sous Linux : d'un fichier .RPM

Tableau 25 : GALSS : Procédure d'installation

Voir en annexe deux exemples de fichiers galss.ini

11.4 Installation de la Cryptolib CPS

La procédure d'installation de la Cryptolib CPS est la suivante :

<table>
<tr><th>#</th><th colspan="3">Cryptolib CPS : Procédure d'installation</th></tr>
<tr><td>1</td><td colspan="3">Appliquer la procédure « GALSS : Procédure d'installation »

✍ Rappel : la procédure « GALSS : Procédure d'installation » ne s'applique pas avec la Cryptolib CPS v4 Full PC/SC</td></tr>
<tr><td>2</td><td colspan="3">Télécharger les derniers composants logiciels, dont le GALSS</td></tr>
<tr><td>3</td><td colspan="3">Connecter le/les lecteur(s) de cartes au poste de poste de travail</td></tr>
<tr><td rowspan="7">4</td><td colspan="3">Démarrer l'installation</td></tr>
<tr><td rowspan="2">Windows</td><td>v4, v5</td><td>lancer « CryptolibCPS-x.y.z.msi »</td></tr>
<tr><td>v4 Full PC/SC</td><td>lancer « SetupCryptoCpsPcsc.vx.yz.msi »</td></tr>
<tr><td rowspan="3">Linux</td><td colspan="2">en mode console, exécuter :</td></tr>
<tr><td>dpkg</td><td>#untar
[sudo] tar xvzf CryptolibCPS-x.y.z-i386.rpm.tar.gz

#Conversion du .rpm en un .deb
[sudo] apt-get install alien
[sudo] alien -k -c CryptolibCPS-x.y.z-i386.rpm

#install
[sudo] dpkg -D 3777 -i cryptolibcps_x.y.z-1_i386.deb > /tmp/logs-cryptolibcps-install.txt 2>&1</td></tr>
<tr><td>rpm</td><td>#untar
[sudo] tar xvzf CryptolibCPS-x.y.z-i386.rpm.tar.gz

#install
[sudo] rpm -i[vh] CryptolibCPS-x.y.z-i386.rpm</td></tr>
<tr><td>Mac OS X</td><td colspan="2">• ouvrir « CryptolibCPS-x.y.z.dmg »
• lancer « CryptolibCPS-x.y.z.pkg »</td></tr>
</table>

#	Cryptolib CPS : Procédure d'installation	
5	Windows	l'installation se termine parfois par un message de demande de redémarrage.
6	Accepter le redémarrage de la machine s'il est demandé	
7	Redémarrer de la machine	
8	Droits	Le compte de l'utilisateur qui va utiliser la Cryptolib CPS doit posséder les droits en lecture et en écriture sur les répertoires suivants et leurs sous-répertoires
	Windows	%ALLUSERSPROFILE%\santesocial\CPS\
	Mac OS X	/Library/Logs/santesocial/CPS/
	Linux	/etc/opt/santesocial/CPS/

Tableau 26 : Cryptolib CPS : Procédure d'installation

Si l'installation s'est bien terminée, les composants logiciels sont maintenant disponibles sur la machine.

En environnement Windows (sauf pour la Cryptolib CPS v4 Full PC/SC, cf. présentation du CCM ci-après), l'icône du programme CCM avec une couleur jaune bordée de vert doit être présente, comme indiqué sur la figure ci-dessous:

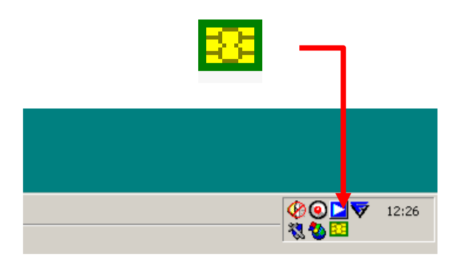


Figure 7 : CCM : Exemple de barre des tâches sous Windows avec CCM en état 1

Pour les autres environnements Linux et Mac, aucun élément visible de ce type n'est à contrôler.

La phase d'installation est terminée.

La phase de vérification de l'installation peut commencer.

12Vérifications de l'installation avec CPS-Gestion

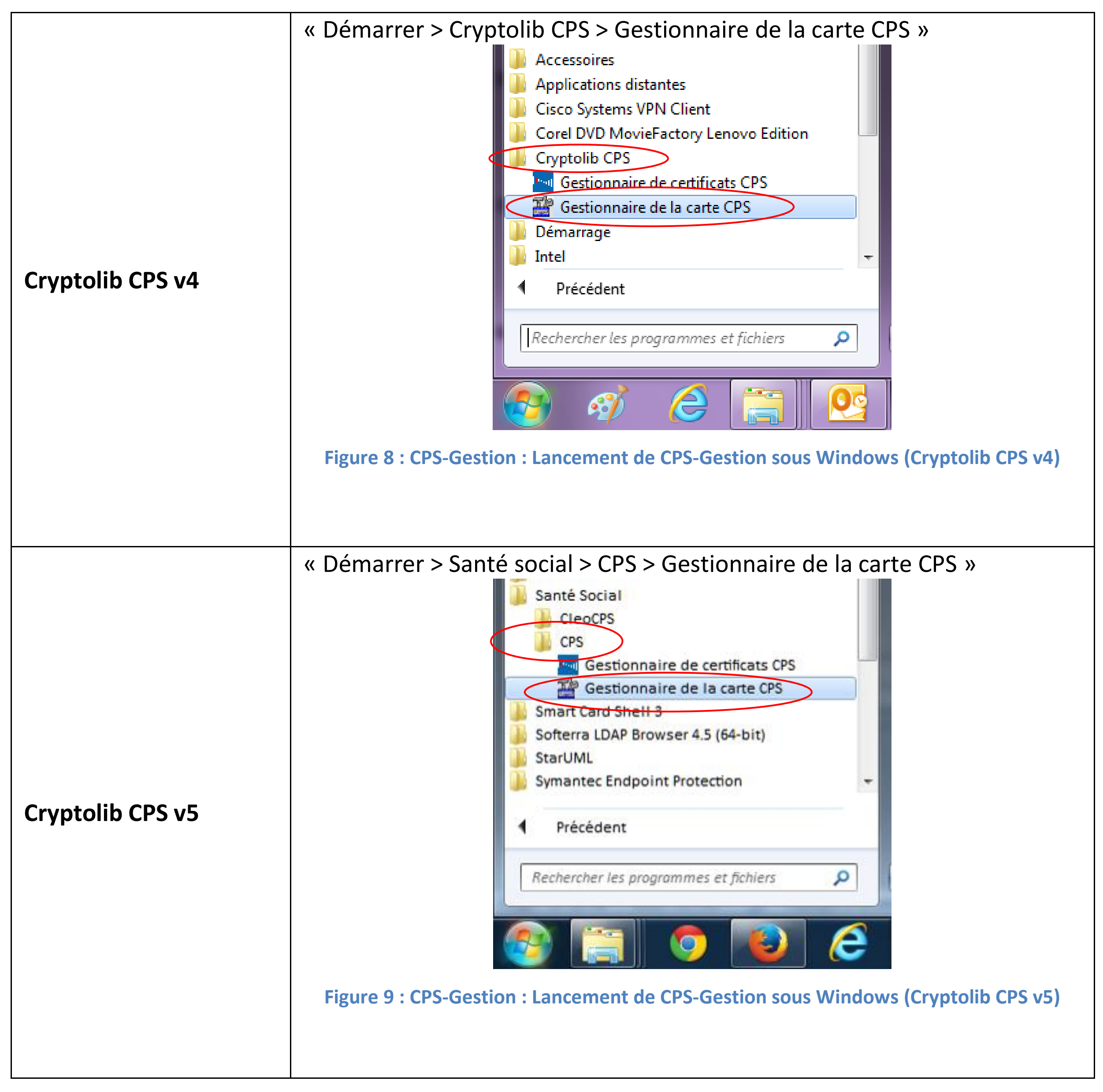
12.1 Présentation de CPS-Gestion

CPS-Gestion est un programme distribué par l'ASIP Santé avec la Cryptolib CPS permettant de visualiser le contenu de la carte CPx connectée au poste de travail. Cet outil offre également la possibilité de débloquer ou de changer le code porteur d'une CPx.

CPS-Gestion est particulièrement utile au moment de tester l'installation de la Cryptolib CPS sur poste de travail.

CPS-Gestion est disponible sous tous les systèmes d'exploitation.

Sous Windows par exemple, CPS-Gestion est accessible depuis le menu **Démarrer** :



Cryptolib CPS v4	« Démarrer > Cryptolib CPS > Gestionnaire de la carte CPS » Figure 8 : CPS-Gestion : Lancement de CPS-Gestion sous Windows (Cryptolib CPS v4)
Cryptolib CPS v5	« Démarrer > Santé social > CPS > Gestionnaire de la carte CPS » Figure 9 : CPS-Gestion : Lancement de CPS-Gestion sous Windows (Cryptolib CPS v5)

Tableau 27 : CPS-Gestion : Lancement sous Windows

12.2 Fonctionnalités de CPS-Gestion

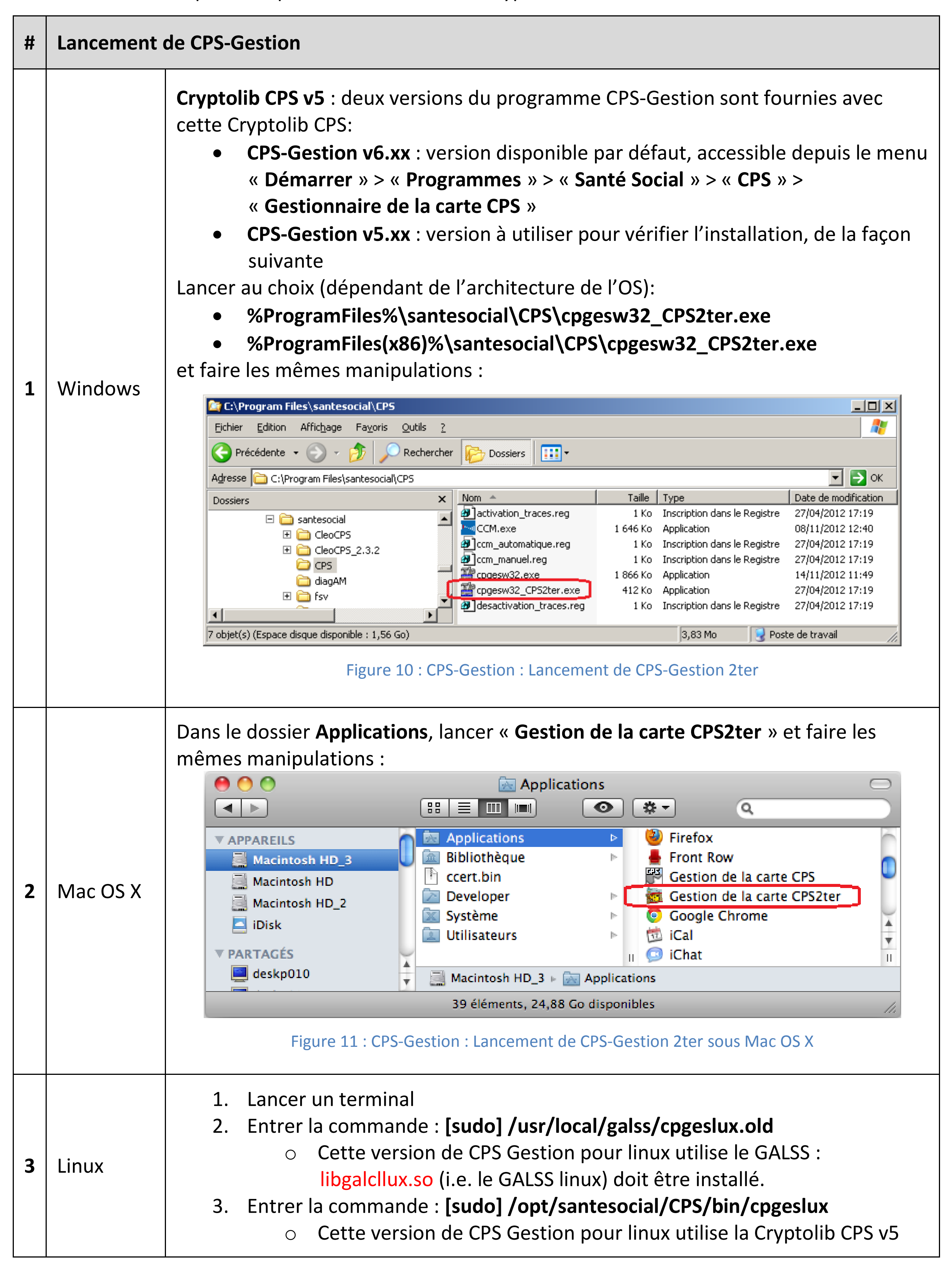
Les fonctionnalités de CPS-Gestion sont accessibles via le menu supérieur et sont les suivantes :

#	Catégorie	Fonctionnalité	Commentaires
1	Gestion lecteur	Test de lecteur	
2		Changement de lecteur	
3	Gestion carte	Changement de carte dans le lecteur	
4		Saisie de code porteur	
5		Changement de code porteur	
6		Déblocage de code porteur	
7	Services CPS	Lecture de données	
8		Lecture et enregistrement X.509	
9		Lecture Situation	
10		Tests des services	
11	Affichage et sauvegarde	Journal	CPS-JOUR.TXT
12		Données CPS	CPS-INFO.TXT
13		Diagnostics	CPS-DIAG.TXT
14		Traces	CPS-TRAC.TXT

Tableau 28 : CPS-Gestion : Liste des fonctionnalités

12.3 Lancement de CPS-Gestion

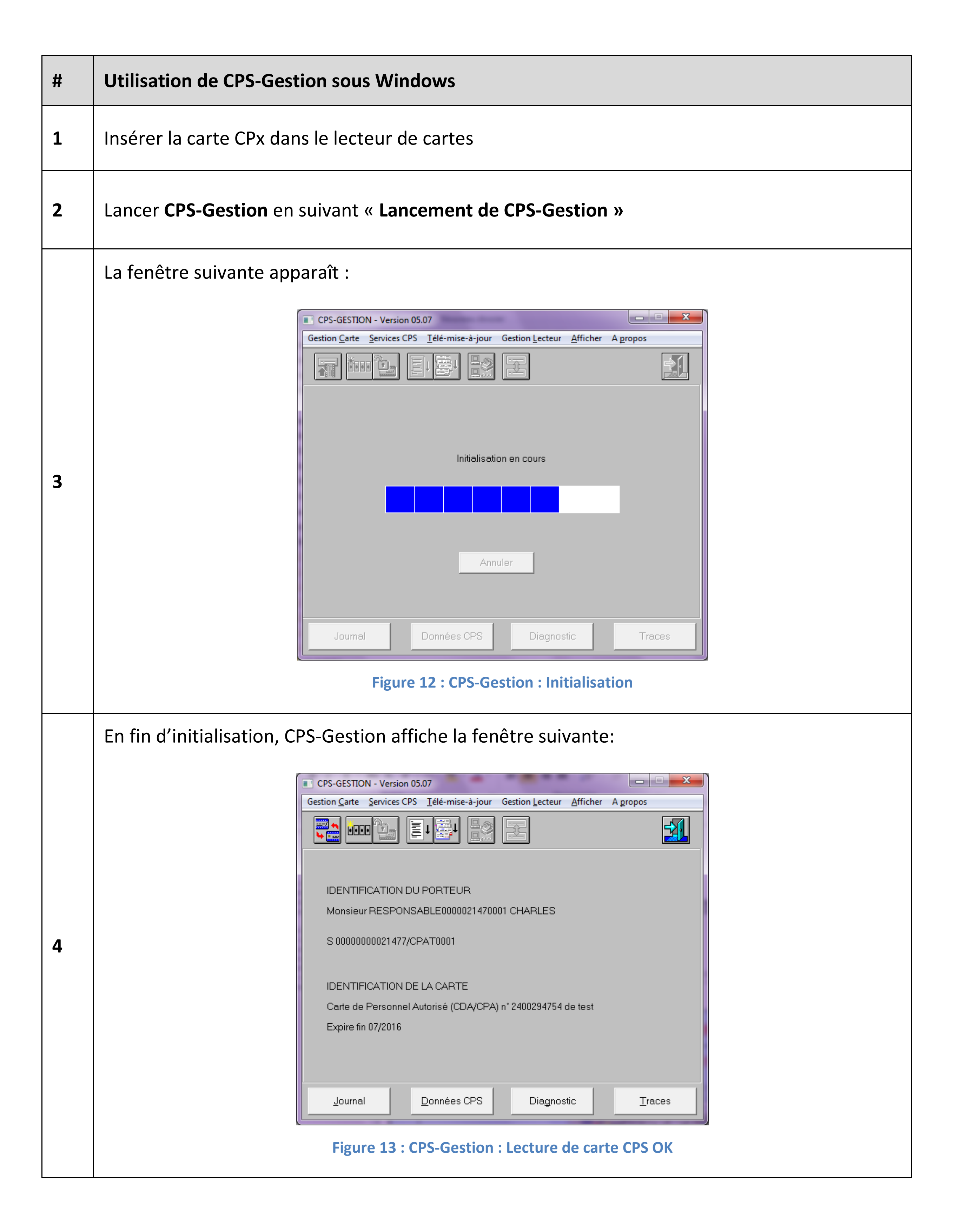
CPS-Gestion est disponible après l'installation de la Cryptolib CPS.



#	Lancement de CPS-Gestion	
1	Windows	**Cryptolib CPS v5** : deux versions du programme CPS-Gestion sont fournies avec cette Cryptolib CPS: • **CPS-Gestion v6.xx** : version disponible par défaut, accessible depuis le menu « **Démarrer** » > « **Programmes** » > « **Santé Social** » > « **CPS** » > « **Gestionnaire de la carte CPS** » • **CPS-Gestion v5.xx** : version à utiliser pour vérifier l'installation, de la façon suivante Lancer au choix (dépendant de l'architecture de l'OS): • **%ProgramFiles%\santesocial\CPS\cpgesw32_CPS2ter.exe** • **%ProgramFiles(x86)%\santesocial\CPS\cpgesw32_CPS2ter.exe** et faire les mêmes manipulations : Figure 10 : CPS-Gestion : Lancement de CPS-Gestion 2ter
2	Mac OS X	Dans le dossier **Applications**, lancer « **Gestion de la carte CPS2ter** » et faire les mêmes manipulations : Figure 11 : CPS-Gestion : Lancement de CPS-Gestion 2ter sous Mac OS X
3	Linux	1. Lancer un terminal 2. Entrer la commande : **[sudo] /usr/local/galss/cpgeslux.old** ○ Cette version de CPS Gestion pour linux utilise le GALSS : libgalcllux.so (i.e. le GALSS linux) doit être installé. 3. Entrer la commande : **[sudo] /opt/santesocial/CPS/bin/cpgeslux** ○ Cette version de CPS Gestion pour linux utilise la Cryptolib CPS v5

Tableau 29 : CPS-Gestion : Lancement de CPS-Gestion

12.4 Utilisation de CPS-Gestion sous Windows



#	Utilisation de CPS-Gestion sous Windows
1	Insérer la carte CPx dans le lecteur de cartes
2	Lancer **CPS-Gestion** en suivant « **Lancement de CPS-Gestion »**
3	La fenêtre suivante apparaît : Figure 12 : CPS-Gestion : Initialisation
4	En fin d'initialisation, CPS-Gestion affiche la fenêtre suivante: Figure 13 : CPS-Gestion : Lecture de carte CPS OK

#	Utilisation de CPS-Gestion sous Windows
5	Faire un « Tests des services » : Figure 14 : CPS-Gestion : Lancement des Tests des services Le code porteur est demandé : Figure 15 : CPS-Gestion : Saisie du code porteur Les tests se déroulent : Figure 16 : CPS-Gestion : Déroulement des tests des services Un résumé (Diagnostic) du résultat des tests est affiché : Figure 17 : CPS-Gestion : Résumé du résultat des tests des services

#	Utilisation de CPS-Gestion sous Windows
6	Ce résultat pourra être demandé dans le cadre du support technique. Pour le récupérer, quitter CPS-Gestion, cocher les 4 fichiers à sauvegarder, puis valider:

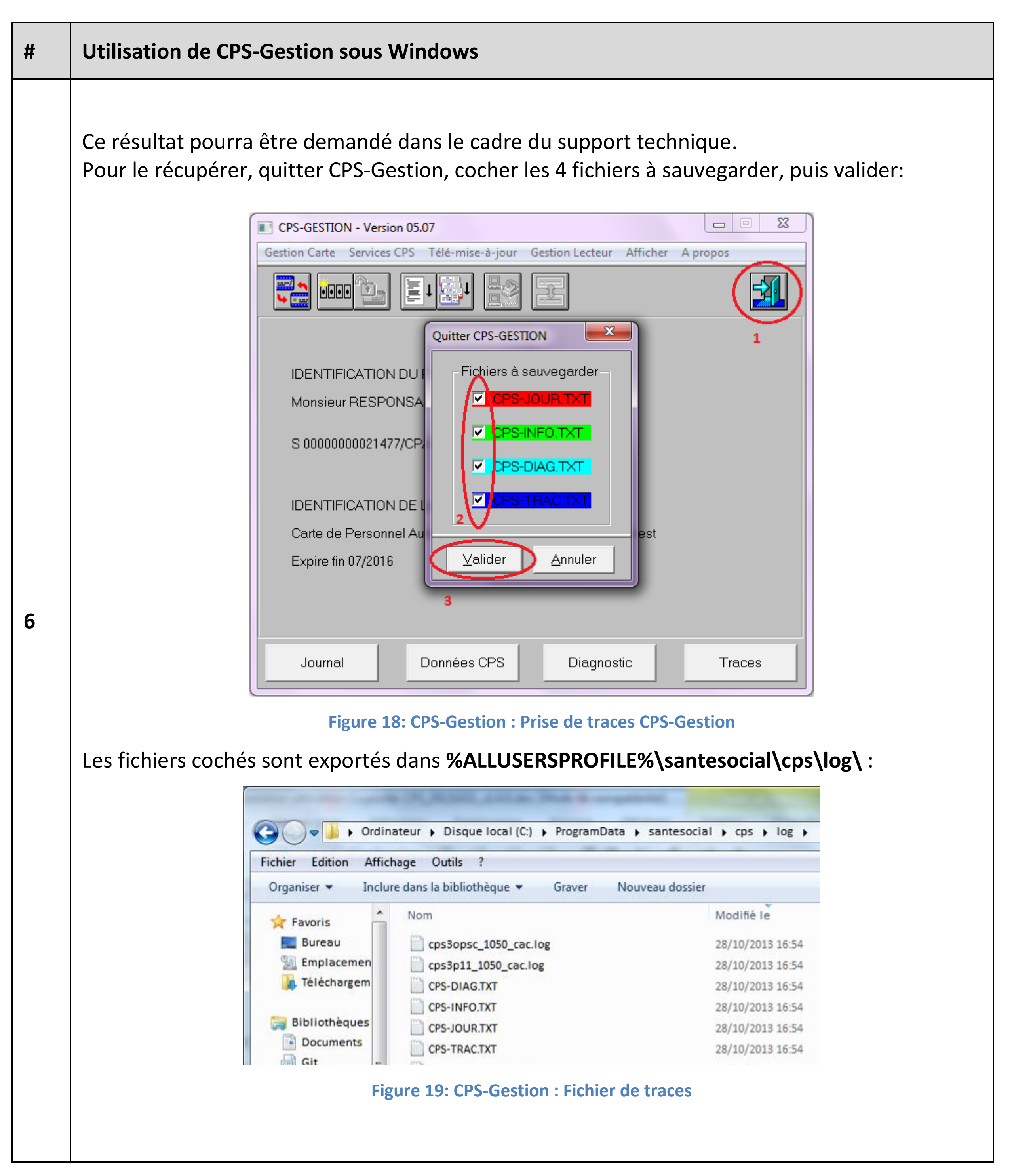


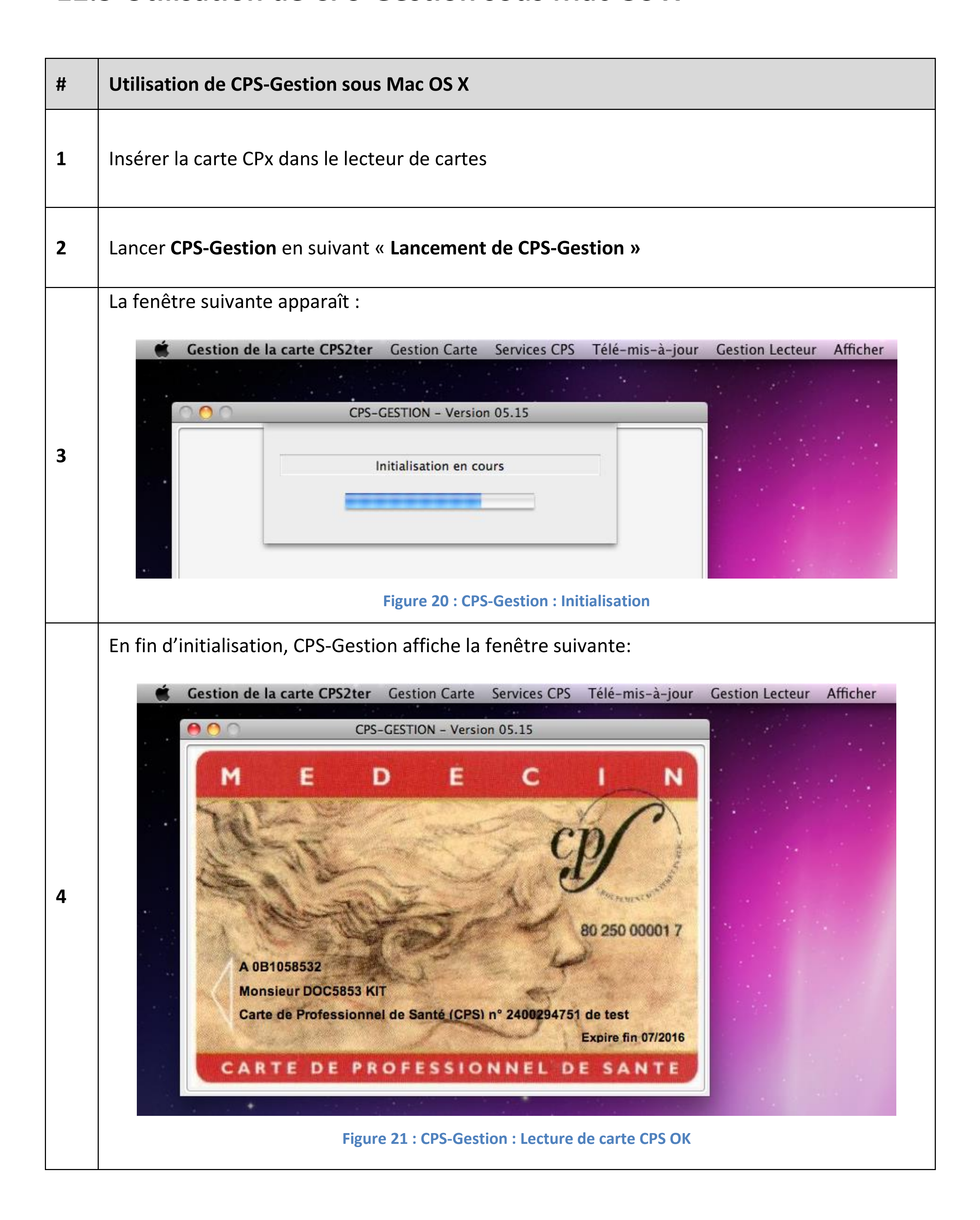
Figure 18: CPS-Gestion : Prise de traces CPS-Gestion

Les fichiers cochés sont exportés dans **%ALLUSERSPROFILE%\santesocial\cps\log** :

Figure 19: CPS-Gestion : Fichier de traces

Tableau 30 : CPS-Gestion : Utilisation pour vérification de l'installation de la Cryptolib CPS

12.5 Utilisation de CPS-Gestion sous Mac OS X

#	Utilisation de CPS-Gestion sous Mac OS X
1	Insérer la carte CPx dans le lecteur de cartes
2	Lancer **CPS-Gestion** en suivant « **Lancement de CPS-Gestion »**
3	La fenêtre suivante apparaît :  Figure 20 : CPS-Gestion : Initialisation
4	En fin d'initialisation, CPS-Gestion affiche la fenêtre suivante: Figure 21 : CPS-Gestion : Lecture de carte CPS OK

#	Utilisation de CPS-Gestion sous Mac OS X
5	Faire un « Tests des services » : Figure 22 : CPS-Gestion : Lancement des Tests des services Le code porteur est demandé : Figure 23 : CPS-Gestion : Saisie du code porteur Les tests se déroulent : Figure 24 : CPS-Gestion : Déroulement des Tests des services Un résumé (Diagnostic) du résultat des tests est affiché : Figure 25 : CPS-Gestion : Résumé du résultat des tests des services

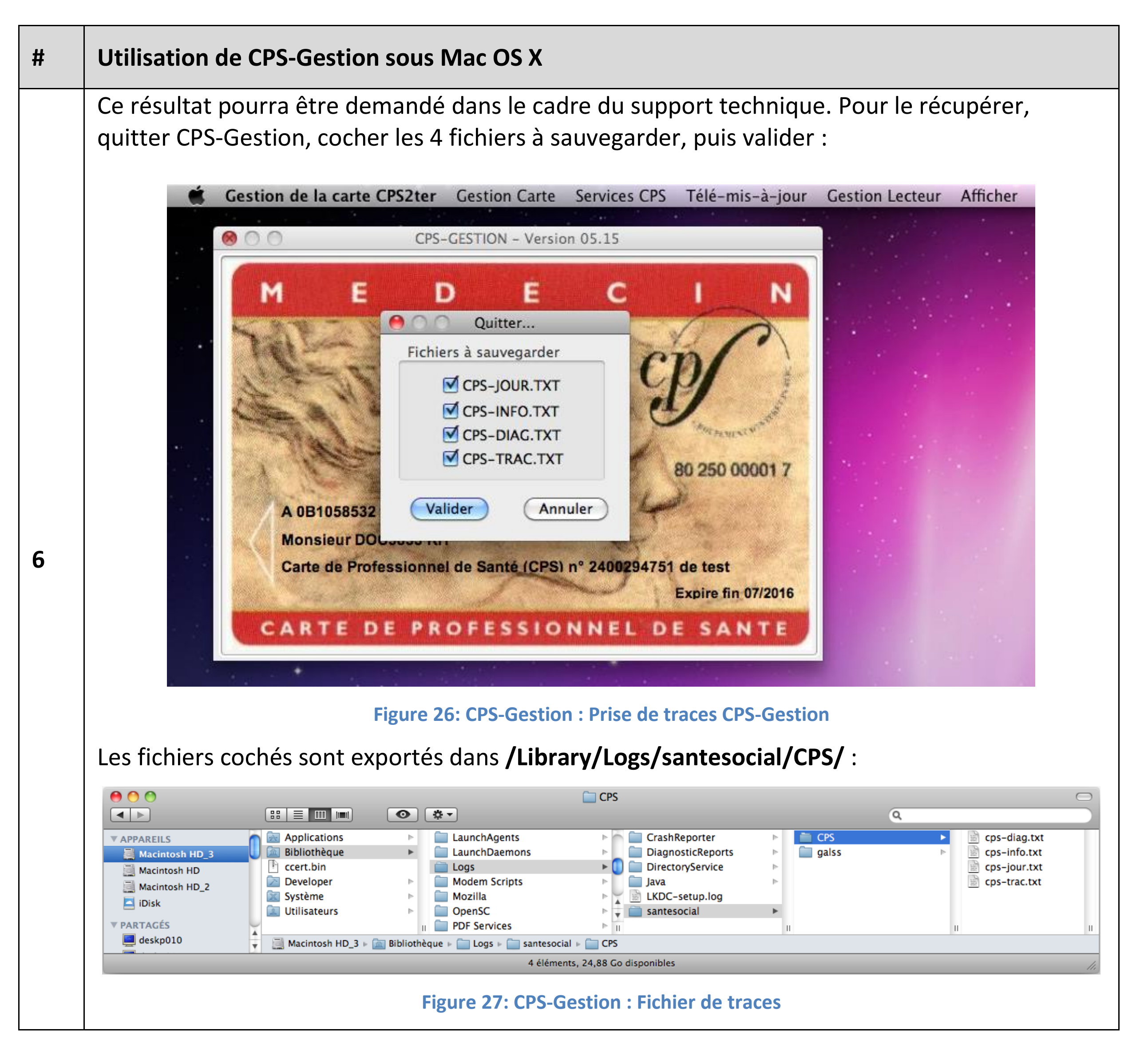
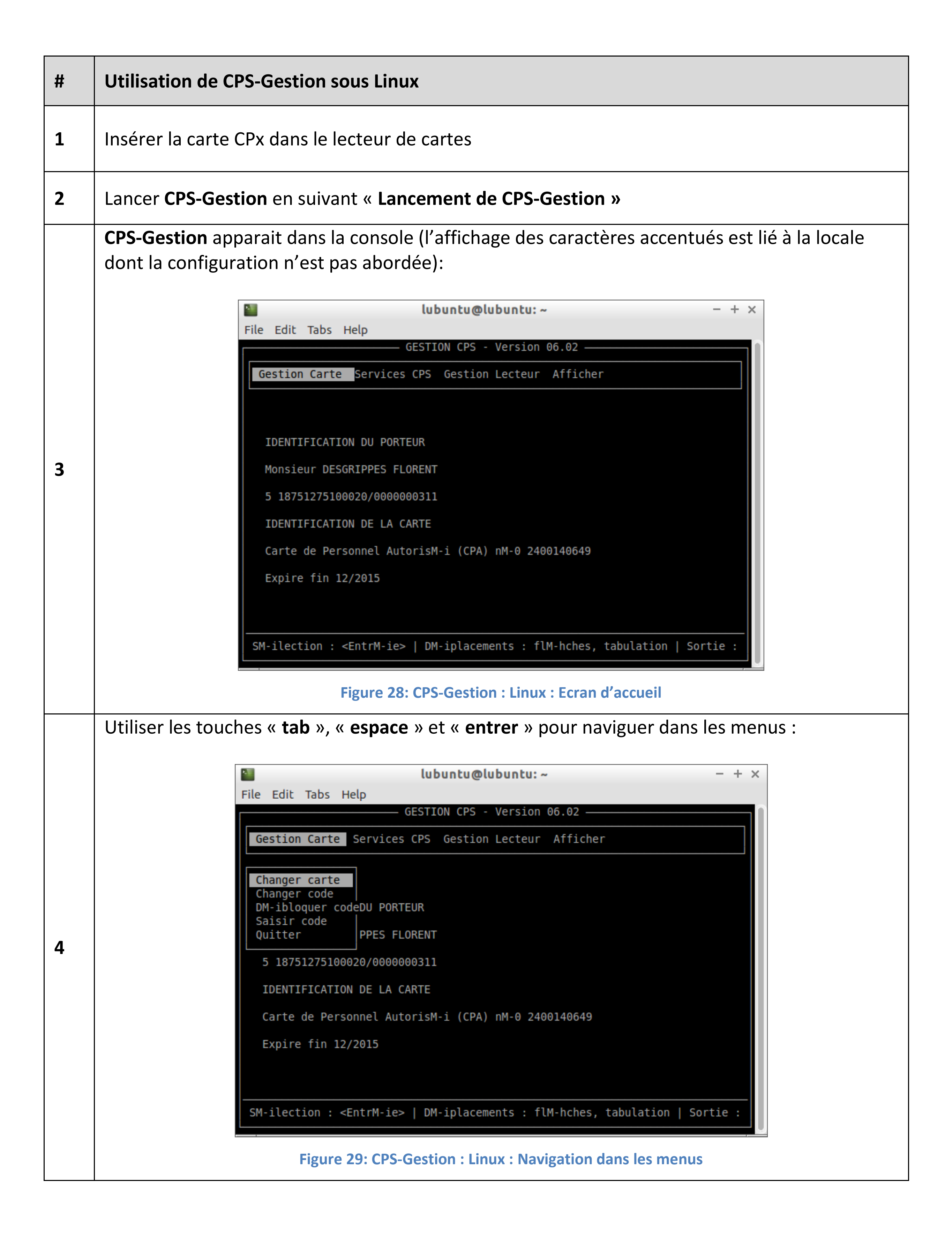
#	Utilisation de CPS-Gestion sous Mac OS X
6	Ce résultat pourra être demandé dans le cadre du support technique. Pour le récupérer, quitter CPS-Gestion, cocher les 4 fichiers à sauvegarder, puis valider :  Figure 26: CPS-Gestion : Prise de traces CPS-Gestion Les fichiers cochés sont exportés dans **/Library/Logs/santesocial/CPS/** : Figure 27: CPS-Gestion : Fichier de traces

Tableau 31 : Utilisation de CPS-Gestion sous Mac OS X

12.6 Utilisation de CPS-Gestion sous Linux



#	**Utilisation de CPS-Gestion sous Linux**
1	Insérer la carte CPx dans le lecteur de cartes
2	Lancer **CPS-Gestion** en suivant « **Lancement de CPS-Gestion »**
3	**CPS-Gestion** apparait dans la console (l'affichage des caractères accentués est lié à la locale dont la configuration n'est pas abordée): Figure 28: CPS-Gestion : Linux : Ecran d'accueil
4	Utiliser les touches « **tab** », « **espace** » et « **entrer** » pour naviguer dans les menus : Figure 29: CPS-Gestion : Linux : Navigation dans les menus

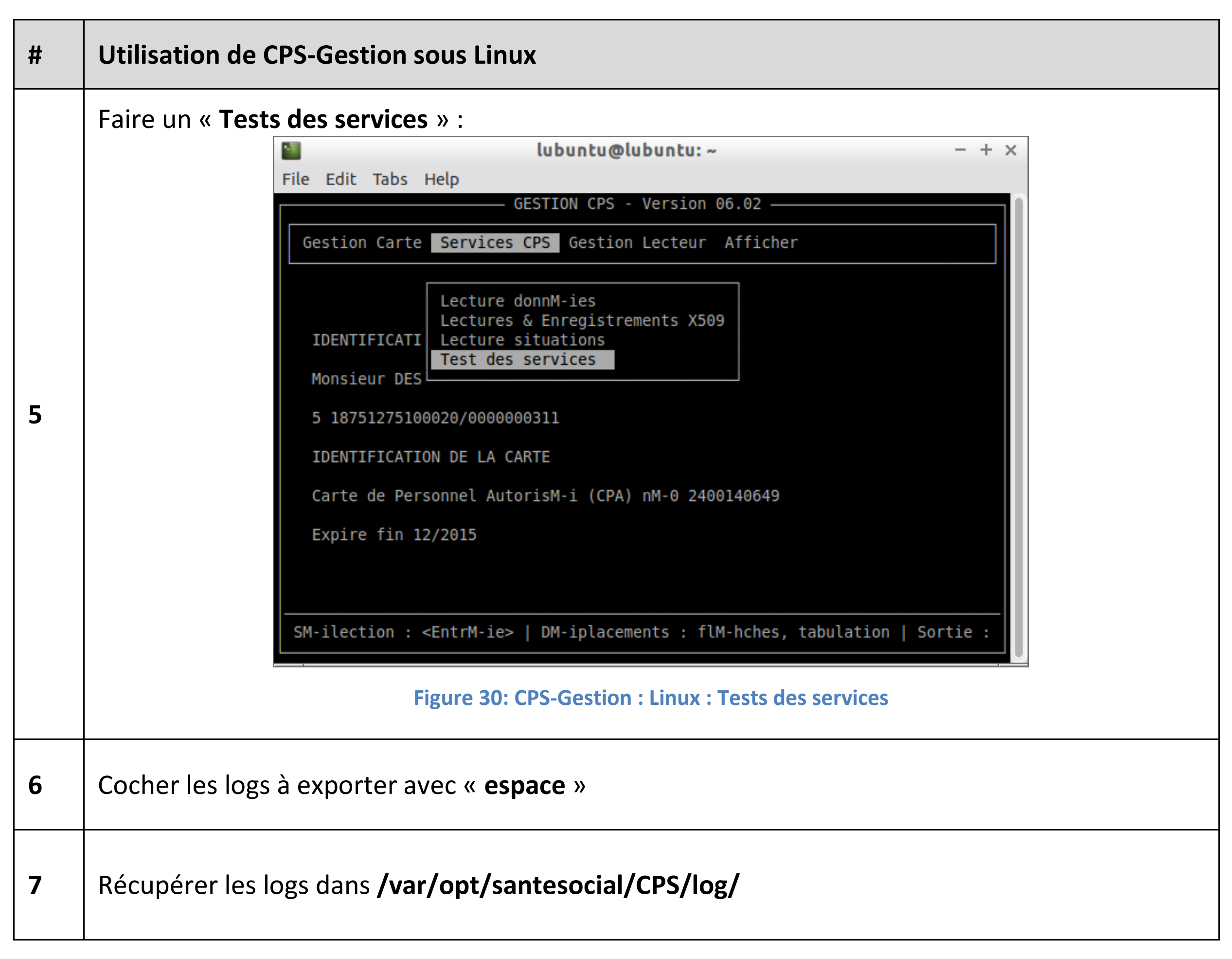
#	Utilisation de CPS-Gestion sous Linux
5	Faire un « **Tests des services** » :  Figure 30: CPS-Gestion : Linux : Tests des services
6	Cocher les logs à exporter avec « **espace** »
7	Récupérer les logs dans **/var/opt/santesocial/CPS/log/**

Tableau 32 : Utilisation de CPS-Gestion sous Linux

13 Premières utilisations

13.1 Premières utilisations sous Microsoft Windows

13.1.1 Le magasin de certificats Windows

13.1.1.1 Rôle du Magasin Windows

Le magasin de certificats est un composant essentiel du système Microsoft Windows.

Il contient les certificats logiciels apportés lors de l'installation de Windows (certificats racine Verisign, Thawte…).

Il contiendra les certificats d'authentification et de signature de la carte CPx du porteur (cf. annexe IGC Santé et certificat X.509).

L'alimentation du magasin de certificats Windows avec ces deux certificats est une tâche indispensable si la carte CPx est destinée à être mise en œuvre avec Internet Explorer ou Outlook par exemple, ou avec toute autre application exploitant les mécanismes cryptographiques spécifiés par Microsoft.

13.1.1.2 Visualisation du contenu du Magasin Windows

Pour visualiser le magasin de certificats Microsoft Windows:

- lancer **Internet Explorer**
- sélectionner le menu « **Outils** », puis « **Options internet** »
- dans l'onglet « **Contenu** », cliquer sur le bouton « **Certificats** ».

La fenêtre suivante apparaît et affiche le magasin des certificats personnels de l'utilisateur :

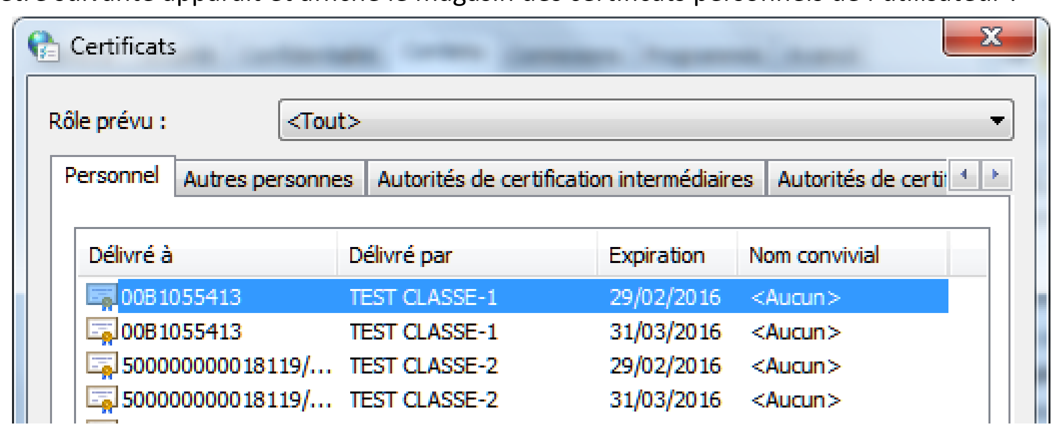


Figure 31 : Windows : Affichage du contenu du Magasin de certificats Windows

13.1.1.3 L’alimentation du Magasin Windows

L’API CryptoAPI / CSP de Microsoft impose aux applications de consulter le magasin de certificat avant de déclencher les opérations cryptographiques mettant en jeu les objets qu’il contient.

Le CSP ASIP Santé, fourni par la Cryptolib CPS, remonte donc les certificats X.509 vers le magasin afin que les applications puissent solliciter les objets qu’il contient.

Cette tâche est effectuée en tâche de fond, soit:

- à intervalles réguliers
  - en particulier si le lecteur est un lecteur PSS
- sur l’évènement d’insertion carte dans le lecteur
  - en particulier si le lecteur est PC/SC

A titre de comparaison, le standard PKCS#11 prévoit un renvoi des certificats X.509 aux applications quand celles-ci les sollicitent. Voir la section « **Architecture** » pour plus de précisions.

13.1.1.4 Le CCM

La tâche de fond d’alimentation du magasin en certificats CPx implique la mise en œuvre d’une fonction de surveillance de la présence d’une carte CPx dans le lecteur.

Cette tâche est assurée par un utilitaire appelé **CCM** fourni par la Cryptolib CPS.

Le couple {CCM, CSP ASIP Santé} assure la cohérence entre l’état du magasin de certificats Microsoft et la présence/absence de la carte CPx dans le lecteur:

- Si une carte CPx est introduite dans un lecteur connecté au poste
  - le CCM détecte l’introduction de la carte
- Si une carte CPx est retirée d’un lecteur connecté au poste
  - le CCM détecte le retrait de la carte
- Dans tous les cas, suite à la détection de l’événement carte par le CCM :
  - le CCM vérifie l’état des lecteurs et des cartes
  - le CCM signale au CSP l’évènement
  - le CSP efface les certificats ASIP Santé présents dans le magasin de certificats personnels
  - le CSP ajoute les certificats associés des cartes encore présentes au magasin de certificats personnels

Windows	Ce programme n'existe que sous Windows
Cryptolib CPS v4 Full PC/SC	Cet utilitaire s'appelle **cps_ccm_pcsc.exe** dans la Cryptolib CPS v4 Full PC/SC. Il tourne en tâche de fond mais ne présente aucune interface graphique (pas d'icône dans la barre de tâche)

Tableau 33 : CCM : Remarques

Lors de l'installation, le programme CCM.exe est ajouté à la liste des programmes devant être lancés au démarrage du poste

- via le raccourci « **Démarrage du CCM** »
- placé dans **%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup**

Le programme est également présent dans le menu :

- **Cryptolib CPS v4** : « Démarrer » > « Programmes » > « Cryptolib CPS »
- **Cryptolib CPS v5** : « Démarrer » > « Programmes » > « Santé Social » > « CPS »

sous le nom « **Gestionnaire de certificats CPS** ».

Au lancement, le CCM signale sa présence par une icône reflétant l'état du lecteur de carte CPS. L'activité de CCM est matérialisée par la présence sur la barre des tâches d'une icône spécifique :

Etat	Icône	Description	Signification
1		Cadre vert	Une carte CPS est présente dans le lecteur. Ses certificats X.509 ont été recopiés dans le magasin Microsoft.
2		Cadre jaune/orange clignotant	La carte CPS est en cours de lecture (état transitoire). Les certificats sont en cours de copie dans le magasin Microsoft.
3		Cadre rouge	Au choix : **1** Pas (ou plus) de carte CPS présente dans le lecteur **2** Problème dans la configuration du poste empêchant l'accès au lecteur de cartes Dans les 2 cas, les certificats ont été effacés du magasin.

Tableau 34 : CCM : Activité du CCM

Voir l'annexe « **Windows 7 et icônes de barre de tâche** » pour une configuration adéquate de l'icône du CCM sous Windows 7.

Tableau 35 : CCM : configuration adéquate de l'icône du CCM sous Windows 7

13.1.1.5 Fonctions de l'interface graphique du CCM

Le CCM est doté d'un menu contextuel (**« clic droit » sur l'icône**) permettant de le configurer ou d'obtenir des informations sur ce dernier. Les menus affichés sont les suivants :

<table>
<tr><th>ID</th><th>Fonction</th><th colspan="3">Description</th></tr>
<tr><td>1</td><td>A propos de CCM…</td><td colspan="3">Affiche les informations sur le programme CCM.</td></tr>
<tr><td>2</td><td>Rafraîchir</td><td colspan="3">Permet de rafraîchir explicitement l'état du lecteur, afin de prendre en compte le retrait/l'insertion d'une carte CPS.
Cette option est à utiliser lorsque le CCM est en mode de surveillance manuelle (surveillance des lecteurs désactivée).</td></tr>
<tr><td rowspan="6">3</td><td rowspan="6">Lister l'état des lecteurs…</td><td colspan="3">Affiche l'état de tous les lecteurs présents et configurés sur le poste.
Figure 32 : CCM : exemple d'état avec un lecteur PC/SC contenant une CPS</td></tr>
<tr><td>Réinitialiser la liste des lecteurs</td><td colspan="2">Permet de prendre en compte le débranchement/rebranchement d'un lecteur sur le poste.</td></tr>
<tr><td rowspan="2">Activer la surveillance des lecteurs</td><td colspan="2">Passage en mode de surveillance automatique : permet de détecter automatiquement le retrait ou l'insertion d'une carte CPS.
Lorsque le basculement à lieu, le bouton change et devient « Désactiver la surveillance des lecteurs ».</td></tr>
<tr><td colspan="2">Ce mode est déconseillé avec les lecteurs PSS</td></tr>
<tr><td>Désactiver la surveillance des lecteurs</td><td colspan="2">Passage en mode de surveillance manuelle : désactive la détection automatique du retrait ou de l'insertion d'une carte CPS.
Lorsque le basculement à lieu, le bouton change et devient « Activer la surveillance des lecteurs ».</td></tr>
<tr><td colspan="3">Dans ce mode, l'utilisateur doit explicitement rafraîchir l'état du lecteur via l'option « Rafraîchir » afin de synchroniser le statut de la carte CPx (présence ou absence dans le lecteur) et le magasin de certificats personnels (présence ou absence des certificats).</td></tr>
</table>

ID	Fonction	Description
		Lors de la première exécution du programme CCM, la surveillance manuelle de l'état du lecteur est activée par défaut.
		Le mode de surveillance (manuelle ou automatique) choisi est reconduit à chaque redémarrage de la machine.
5	**Quitter**	Permet de quitter le programme CCM

Tableau 36 : CCM : Fonctionnalités de l'interface graphique

13.1.1.6 Le service de propagation Microsoft

Le service de propagation de certificat est un service standard sur le système d'exploitation Microsoft Windows depuis les versions Vista.

Il apporte en standard des fonctionnalités offertes jusque-là par le CCM.

Il ne fonctionne qu'avec :

- Les lecteurs PC/SC
  - Il n'est pas mis en œuvre si la carte CPx est insérée dans un lecteur PSS
- La Cryptolib CPS v5

Dans ce cas, il s'exécute en parallèle du CCM.

A la différence du CCM, il n'efface pas les certificats ASIP Santé sur l'événement de retrait de carte du lecteur.

Ce point ne pose aucun problème de sécurité, les certificats X.509 ne contenant que des données publiques non confidentielles (cf. partie « **Sécurité et performances** »).

Ce point peut cependant poser problème en utilisation avec les LPS qui présupposaient généralement jusque-là qu'il n'y avait que la paire de certificats de la carte courante en magasin.

L'utilisation du CCM reste donc préconisée sous les versions de Windows supérieures ou égales à Windows Vista pour deux raisons principales : • Compatibilité des LPS vis à vis de la présence de plus de 2 certificats CPx dans le magasin à vérifier • Lecteur PSS non compatible avec le Service de Propagation

Tableau 37 : Préconisations CCM vs service de propagation Windows

13.1.2 Contrôle de l'installation

13.1.2.1 Contrôle de l'état du GALSS

Cette procédure ne s'applique pas avec la Cryptolib CPS v4 Full PC/SC

Cette procédure ne s'applique pas avec la Cryptolib CPS v5 avec lecteurs PC/SC sans GALSS

La première vérification à effectuer consiste à vérifier que le GALSS fonctionne (cf. manuel du GALSS **[6]**). Pour cela :

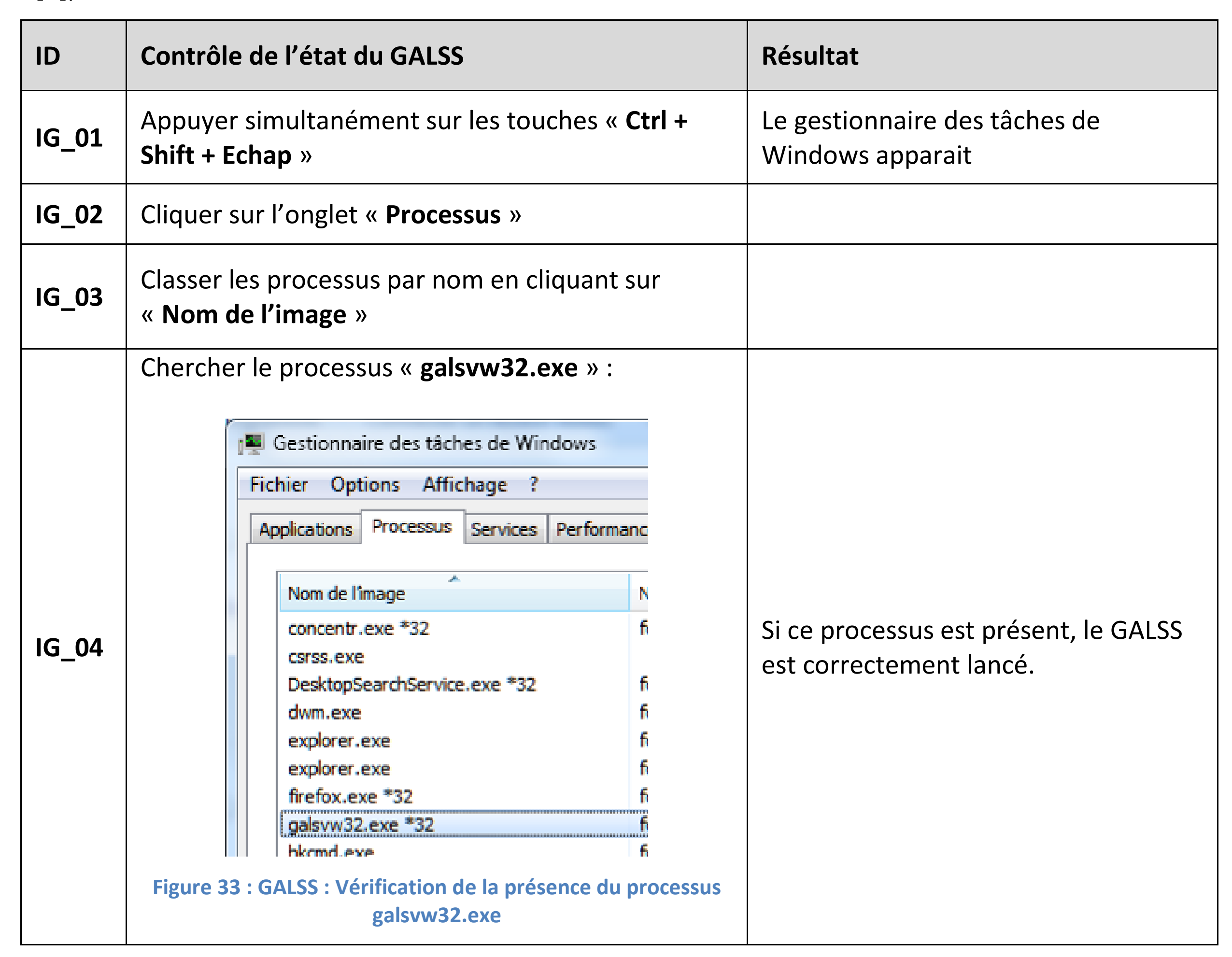
ID	Contrôle de l'état du GALSS	Résultat
IG_01	Appuyer simultanément sur les touches « **Ctrl + Shift + Echap** »	Le gestionnaire des tâches de Windows apparait
IG_02	Cliquer sur l'onglet « **Processus** »	
IG_03	Classer les processus par nom en cliquant sur « **Nom de l'image** »	
IG_04	Chercher le processus « **galsvw32.exe** » :  Figure 33 : GALSS : Vérification de la présence du processus galsvw32.exe	Si ce processus est présent, le GALSS est correctement lancé.

Tableau 38 : Contrôles : Contrôle de l'état du GALSS

ID	Contrôle de l'état du GALSS : Gestion des erreurs	Résultat
IG_81	Vérifier que le lecteur de cartes est branché	
IG_82	Vérifier que la carte est dans le lecteur et sous tension	Dans ce cas, le lecteur affiche généralement une diode lumineuse dans un couleur particulière
IG_83	Relancer la machine	
IG_84	Si le processus GALSS n'est toujours pas présent, même après relance de la machine, passer tout de même à la partie « **Contrôle de l'état du CCM** »	

Tableau 39 : Contrôles : Contrôle de l'état du GALSS : Gestion des erreurs

13.1.2.2 Contrôle de l'état du CCM

La seconde vérification à effectuer est de s'assurer que l'utilitaire CCM a bien détecté la carte CPS dans le lecteur en vérifiant que le **CCM est dans l'état 1 (icône de carte à puce entouré de vert)**.

ID	Contrôle de l'état du CCM	Résultat
IC_01	Appuyer simultanément sur les touches « **Ctrl + Shift + Echap** »	Le gestionnaire des tâches de Windows apparait
IC_02	Cliquer sur l'onglet « **Processus** »	
IC_03	Classer les processus par nom en cliquant sur « **Nom de l'image** »	
IC_04	Chercher le processus « **CCM.exe** » : Figure 34 : CCM : Vérification de la présence du processus CCM.exe	Si le processus est présent, le CCM est correctement lancé.
IC_05	Figure 35 : CCM : Vérification de l'état du CCM	Voir Annexe « **Configuration des icônes de la barre de tâche Windows** » qui décrit les points à configurer en cliquant sur « **Personnaliser…** »

Tableau 40 : Contrôles : Contrôle de l'état du CCM

Si ce n'est pas le cas, deux choix :

ID	Contrôle de l'état du CCM : Gestion des erreurs	Résultat
1- L'icône du CCM n'apparait pas dans la barre de tâche		
IC_81	Vérifier que le lecteur de cartes est branché	
IC_82	Vérifier que la carte est dans le lecteur	
IC_83	Lancer le CCM manuellement	Le programme est présent dans le menu : • **v4** : « **Démarrer** » > « **Programmes** » > « **Cryptolib CPS** » • **v5** : « **Démarrer** » > « **Programmes** » > « **Santé Social** » > « **CPS** » Cliquer sur « **Gestionnaire de certificats CPS** »
IC_84	Revérifier l'état du GALSS en repartant de « **Contrôle de l'état du GALSS** »	Le CCM lance le GALSS si besoin
IC_85	Vérifier que l'icône du CCM apparaît	
IC_86	Si ce n'est pas le cas, redémarrer la machine	Après redémarrage, reprendre les vérifications à partir de « **Contrôle de l'état du GALSS** »
IC_87	Si l'icône du CCM n'apparaît toujours pas, même après plusieurs redémarrages	Contacter le support CPx de l'ASIP Santé
2- L'icône du CCM apparait dans la barre de tâche mais L'état du CCM est différent de 1		
IC_8A	Vérifier que le lecteur de cartes est branché	
IC_8B	Vérifier que la carte est dans le lecteur	
IC_8C	Redémarrer la machine	Après redémarrage, reprendre les vérifications à partir de « **Contrôle de l'état du GALSS** »
IC_8D	Si l'icône du CCM ne passe pas au vert, même après redémarrage	Il peut s'agir d'un problème de droits : • Le compte utilisé doit avoir le droit de lancer des processus GALSS • Le compte utilisé doit avoir suffisamment de droits en lecture / écriture (voir plus loin)

<table>
<tr><th>ID</th><th>Contrôle de l'état du CCM : Gestion des erreurs</th><th>Résultat</th></tr>
<tr><td>IC_8E</td><td></td><td>Il peut s'agir de <u>problèmes matériels</u> :
• Avec le lecteur
  ○ Utiliser les utilitaires de tests fournis avec le lecteur
• Avec la carte CPx
  ○ Changer de carte
  ○ Mettre la carte dans un autre lecteur/sur une autre machine</td></tr>
<tr><td colspan="3">Cependant, le plus probable est que le fichier galss.ini soit corrompu :</td></tr>
<tr><td colspan="3">Appliquer la procédure de régénération du fichier galss.ini (cf. installation du GALSS plus haut)</td></tr>
<tr><td colspan="3">Si le problème persiste malgré la procédure de régénération du fichier galss.ini :</td></tr>
<tr><td>IC_91</td><td>Si différents fichiers galss.ini existent (cf. liste d'emplacements précisée dans la procédure « GALSS : Procédure de sauvegarde du fichier galss.ini »)</td><td>Les installations et les exécutions ont eu lieu avec différents niveaux d'UAC</td></tr>
<tr><td>IC_92</td><td>Dans ce cas, si un LPS est présent sur le poste</td><td>Contacter le Support éditeur du LPS afin de préciser avec lui les modalités d'exécution de son logiciel</td></tr>
<tr><td>IC_93</td><td>Dans ce cas, comparer les différents fichiers galss.ini existants (cf. liste d'emplacements précisée dans la procédure « GALSS : Procédure de sauvegarde du fichier galss.ini »)</td><td>Les différents fichiers galss.ini doivent être identiques</td></tr>
<tr><td>IC_93</td><td>Si les fichiers ne sont pas identiques</td><td>Contacter un support informatique
• le Support éditeur du LPS
• un Support privé si le poste fait l'objet d'un contrat de maintenance</td></tr>
<tr><td colspan="3">Si le problème persiste :

• le CCM reste au rouge
• malgré un « Contrôle de l'état du GALSS » positif
• malgré la « Procédure de régénération du galss.ini » positif

Contacter le Support CPx de l'ASIP Santé (cf. tableau des services Support en début de document)</td></tr>
</table>

Tableau 41 : Contrôles : Contrôle de l'état du CCM : Gestion des erreurs

13.1.2.3 Contrôle de l'état du Magasin Windows

ID	Contrôle de l'état du Magasin Windows	Résultat
MG_01	Insérer une carte CPx dans le lecteur	
MG_02	Rafraîchir le CCM en cliquant droit sur l'icône du CCM et en choisissant « **Rafraîchir l'état du lecteur »** (voir présentation du CCM plus haut)	
MG_03	Visualiser le magasin de certificats Microsoft Windows: • lancer **Internet Explorer** • sélectionner le menu « **Outils** », puis « **Options internet** » • dans l'onglet « **Contenu** », cliquer sur le bouton « **Certificats** » La fenêtre qui apparaît affiche le magasin des certificats personnels de l'utilisateur	
MG_04	Figure 36 : Windows : Vérification du magasin de certificat	
MG_05	Les deux certificats d'authentification et de signature associés à la carte CPx présente dans le lecteur doivent être présents	

Tableau 42 : Contrôles : Contrôle de l'état du Magasin Windows

ID	Contrôle de l'état du Magasin Windows: Gestion des erreurs	Résultat
MG _81	Vérifier que le lecteur de cartes est bien branché	
MG _82	Vérifier que la carte CPx est bien insérée dans le lecteur	
MG _83	Rafraîchir le CCM en cliquant droit sur l'icône du CCM et en choisissant **Rafraîchir l'état du lecteur**	
MG _84	Vérifier l'état du GALSS (cf. plus haut)	
MG _85	Vérifier l'état du CCM (cf. plus haut)	

Tableau 43 : Contrôles : Contrôle de l'état du Magasin Windows: Gestion des erreurs

13.1.2.4 *Contrôle de Connexion HTTPS*

#	Contrôle de Connexion HTTPS sous Windows avec Internet Explorer
1	Lancer Internet Explorer et saisir dans la zone adresse : • http://testssl.asipsante.fr puis cliquer sur le lien • https://testssl.asipsante.fr
2	Accepter et valider les différentes fenêtres jusqu'à voir celle-ci : Figure 37 : Authentification : Sélection du certificat sous Windows XP Figure 38 : Authentification : Sélection du certificat sous Windows 7 Cette fenêtre correspond au certificat X.509 d'authentification de votre carte CPS.
3	Appuyer sur « Afficher le certificat » pour afficher le détail du certificat.
4	Appuyer sur « OK ».
5	La fenêtre suivante apparaît: Figure 39 : Authentification : Saisie du code porteur avec la Cryptolib CPS v4 GALSS Figure 40 : Authentification : Saisie du code porteur avec la Cryptolib CPS v4 Full PC/SC Figure 41 : Authentification : Saisie du code porteur avec la Cryptolib CPS v5
6	Saisir les 4 chiffres du code porteur de la carte CPS.
7	En cas de succès de l'authentification, la page suivante apparaît:

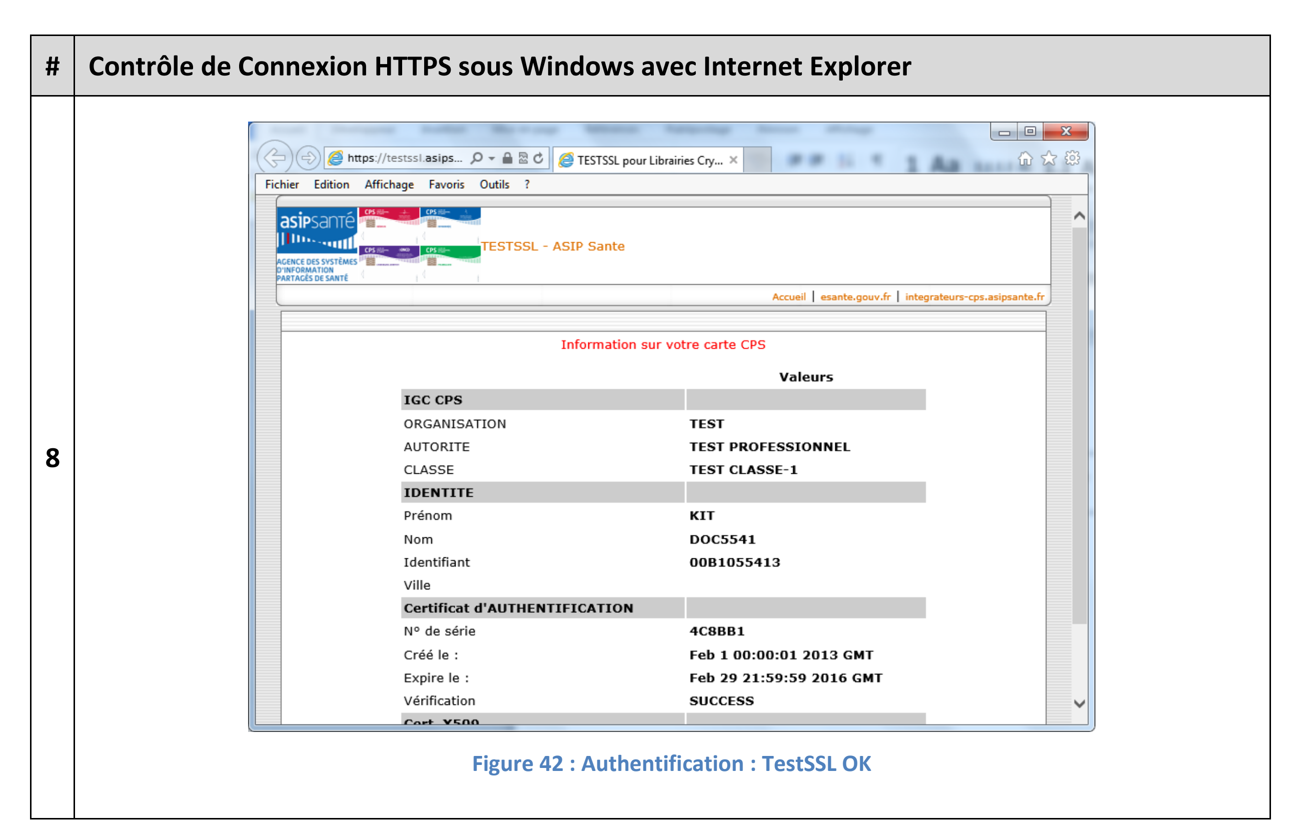
#	Contrôle de Connexion HTTPS sous Windows avec Internet Explorer
8	 Figure 42 : Authentification : TestSSL OK

Tableau 44 : Contrôle de Connexion HTTPS sous Windows avec Internet Explorer

L'apparition de cette page garantit que l'installation des composants logiciels s'est déroulée correctement.

13.2 Premières utilisations sous Apple Mac OS X

13.2.1 Contrôles visuels de l'installation

Une fois l'installation effectuée, il est possible de vérifier le bon fonctionnement du Tokend CDSA (et donc de l'ensemble des éléments installés) à l'aide du programme de visualisation des clés et des certificats inclus dans l'OS.

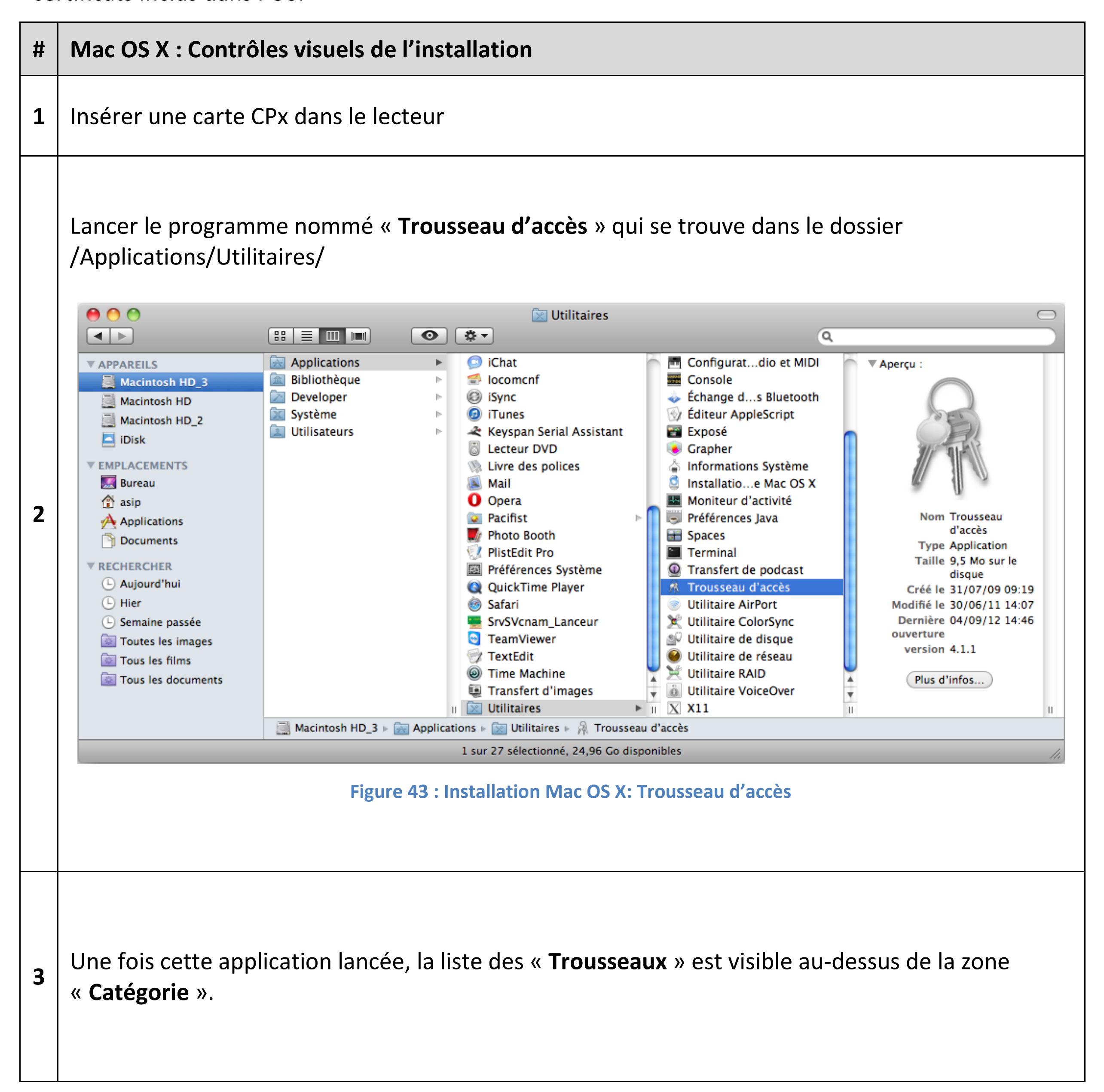
<table>
<tr><th>#</th><th>Mac OS X : Contrôles visuels de l'installation</th></tr>
<tr><td>1</td><td>Insérer une carte CPx dans le lecteur</td></tr>
<tr><td>2</td><td>Lancer le programme nommé « Trousseau d'accès » qui se trouve dans le dossier /Applications/Utilitaires/


Figure 43 : Installation Mac OS X: Trousseau d'accès</td></tr>
<tr><td>3</td><td>Une fois cette application lancée, la liste des « Trousseaux » est visible au-dessus de la zone « Catégorie ».</td></tr>
</table>

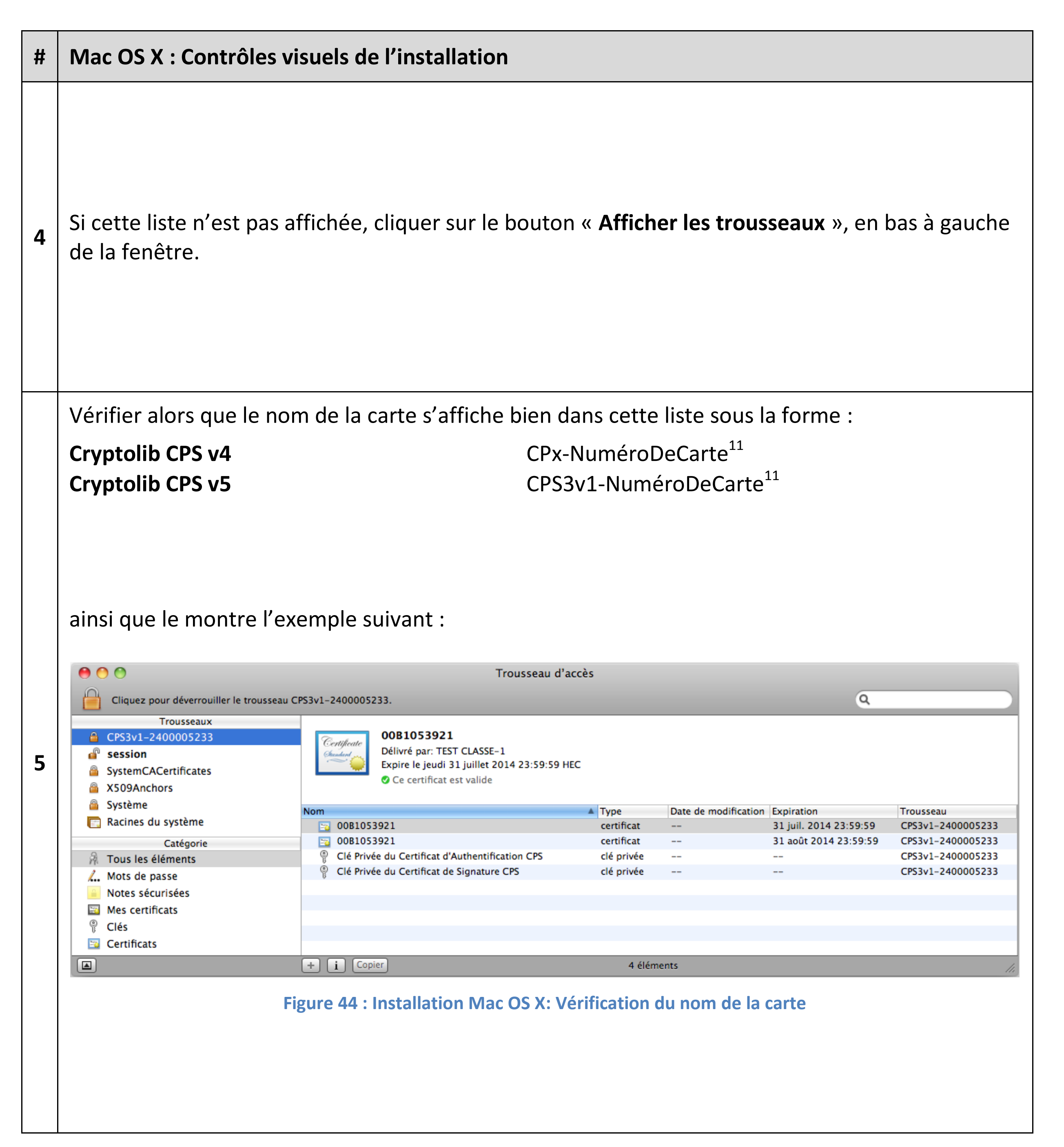
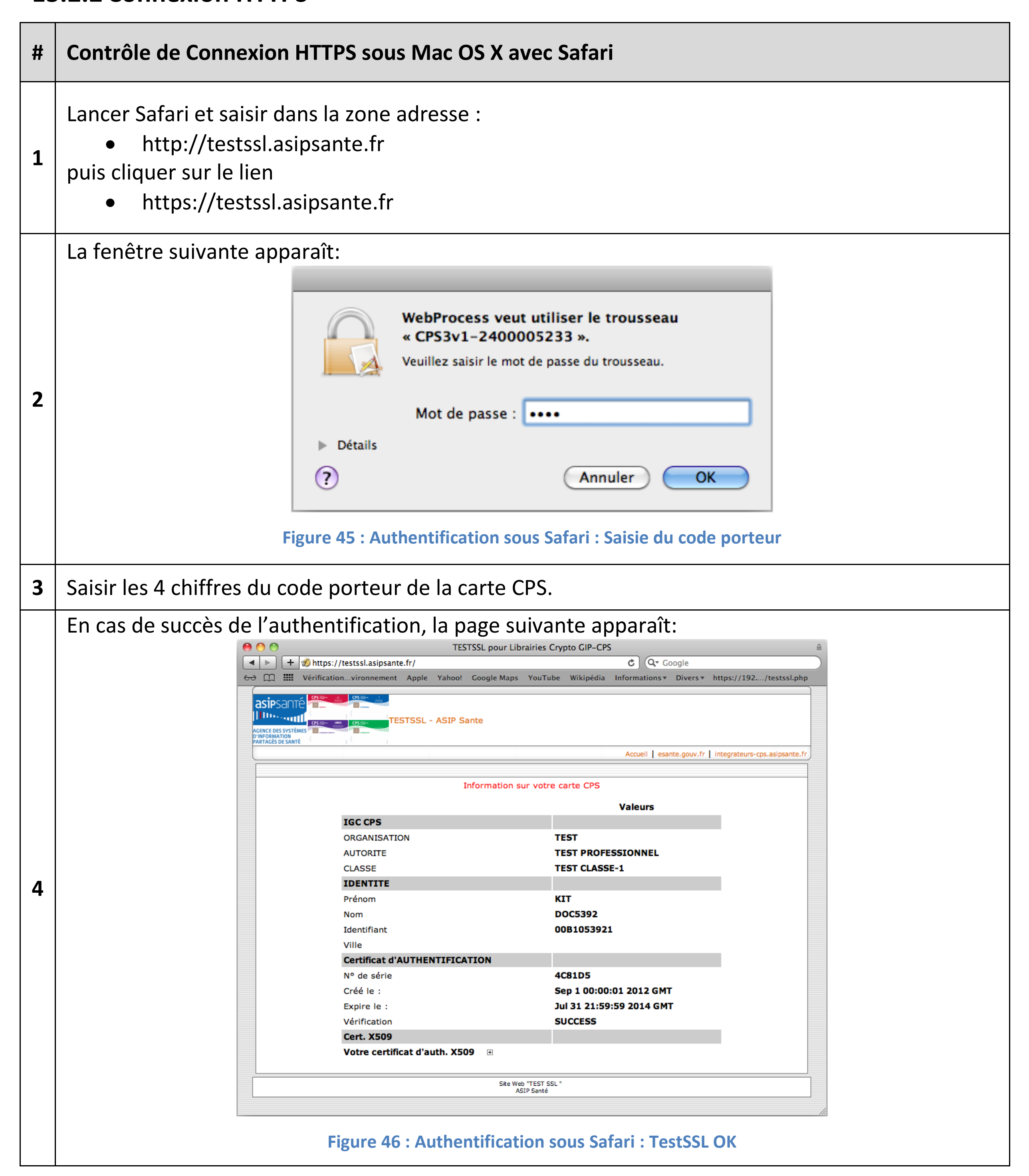
#	Mac OS X : Contrôles visuels de l'installation
4	Si cette liste n'est pas affichée, cliquer sur le bouton « **Afficher les trousseaux** », en bas à gauche de la fenêtre.
5	Vérifier alors que le nom de la carte s'affiche bien dans cette liste sous la forme : **Cryptolib CPS v4** CPx-NuméroDeCarte[11] **Cryptolib CPS v5** CPS3v1-NuméroDeCarte[11] ainsi que le montre l'exemple suivant :  Figure 44 : Installation Mac OS X: Vérification du nom de la carte

Tableau 45 : Mac OS X: Contrôles visuels de l'installation

La présence de ce trousseau indique la bonne installation et le bon fonctionnement de l'ensemble des composants de l'ASIP Santé : la carte a été lue correctement et elle est bien vue comme un Tokend par le système.

[11] NuméroDeCarte = numéro à 10 chiffres inscrit sous le patronyme sur le visuel de la carte.

13.2.2 Connexion HTTPS



#	Contrôle de Connexion HTTPS sous Mac OS X avec Safari
1	Lancer Safari et saisir dans la zone adresse : • http://testssl.asipsante.fr puis cliquer sur le lien • https://testssl.asipsante.fr
2	La fenêtre suivante apparaît: Figure 45 : Authentification sous Safari : Saisie du code porteur
3	Saisir les 4 chiffres du code porteur de la carte CPS.
4	En cas de succès de l'authentification, la page suivante apparaît: Figure 46 : Authentification sous Safari : TestSSL OK

Tableau 46 : Contrôle de Connexion HTTPS sous Mac OS X avec Safari

L'apparition de cette page garantit que l'installation des composants logiciels s'est déroulée correctement.

13.3 Premières utilisations sous Linux

13.3.1 Contrôles de l'installation

Une fois l'installation effectuée, il est possible de vérifier le bon fonctionnement de la Cryptolib CPS sous Linux

#	Linux : Contrôles visuels de l'installation		
1	Lancer **pcscd** en mode debug		sudo systemctl stop pcscd.socket sudo systemctl stop pcscd.service systemctl status pcscd. socket systemctl status pcscd.service sudo pcscd --foreground --debug
2	Insérer une carte CPx dans le lecteur		L'ATR de la carte insérée doit apparaître dans la console pcscd: Figure 47 : Linux : Détection insertion carte par pcscd
3	Rpm		rpm -V CryptoLibCPS-vx.y.z
	Dpkg	vérification de l'activité de dpkg	cat /var/log/dpkg.log
		vérification de l'installation de l'extension Firefox	ls -al /usr/lib/firefox/browser/extensions/
		Consultation des logs de la ligne dpkg -D … > /tmp/logs-cryptolibcps-install.txt 2>&1	cat /tmp/logs-cryptolibcps-install.txt
4	Dpkg	Vérifier le statut du package	sudo dpkg -l cryptolibcps La sortie de cette commande doit contenir les éléments suivants : • ii (install / install / pas d'erreur) • cryptolibcps • x.y.z-1 • i386 • Composants Cryptographiques CPS vx.y.z

#	Linux : Contrôles visuels de l'installation		
		Lister le contenu du package	dpkg -L cryptolibcps Les éléments significatifs sont : /usr/bin/cpgeslux /usr/local/galss/cpgeslux.old /usr/local/galss/libcps_pkcs11_lux.so /usr/local/galss/libcpslux.so /usr/local/galss/libcptablux.so /usr/local/galss/libsscaslux.so /etc/opt/santesocial/CPS/DICO-FR.GIP /etc/opt/santesocial/CPS/cache /etc/opt/santesocial/CPS/cps3_pkcs11.conf /etc/opt/santesocial/CPS/cps_pkcs11_safe.ini /opt/santesocial/CPS/bin/cpgeslux /opt/santesocial/CPS/lib/libcps3_pkcs11_lux.so /usr/lib/libcps3_pkcs11_lux.so /usr/lib/libcps3_pkcs11_lux.so.0 /usr/lib/libcps3_pkcs11_lux.so.1.0.4 /usr/lib/libcps_pkcs11_lux.so /usr/lib/libcptablux.so
5	Lancer CPS-Gestion		
6	Faire un test des services avec CPS-Gestion		

Tableau 47 : Linux: Contrôles de l'installation

13.3.2 Configurations manuelles supplémentaires

SE_Linux	Il peut être nécessaire de passer la commande chcon -t textrel_shlib_t sur les librairies sur un OS Linux avec SE_Linux activé.

13.3.3 Connexions HTTPS

Se rapporter à la section « **Utilisations avec Firefox** ».

14Utilisations avec Firefox

14.1 Utilisations avec Firefox sous Microsoft Windows

14.1.1 Vérification du Module de sécurité CPS

<table>
<tr><th>#</th><th>Firefox : Vérification du Module de sécurité CPS</th></tr>
<tr><td>1</td><td>Fermer toutes les instances de Firefox si cela n'avait pas été fait avant</td></tr>
<tr><td>2</td><td>Relancer le navigateur Firefox</td></tr>
<tr><td>3</td><td>Accepter l'installation de l'extension CPS de l'ASIP Santé pour Firefox en cochant « Autoriser cette installation »

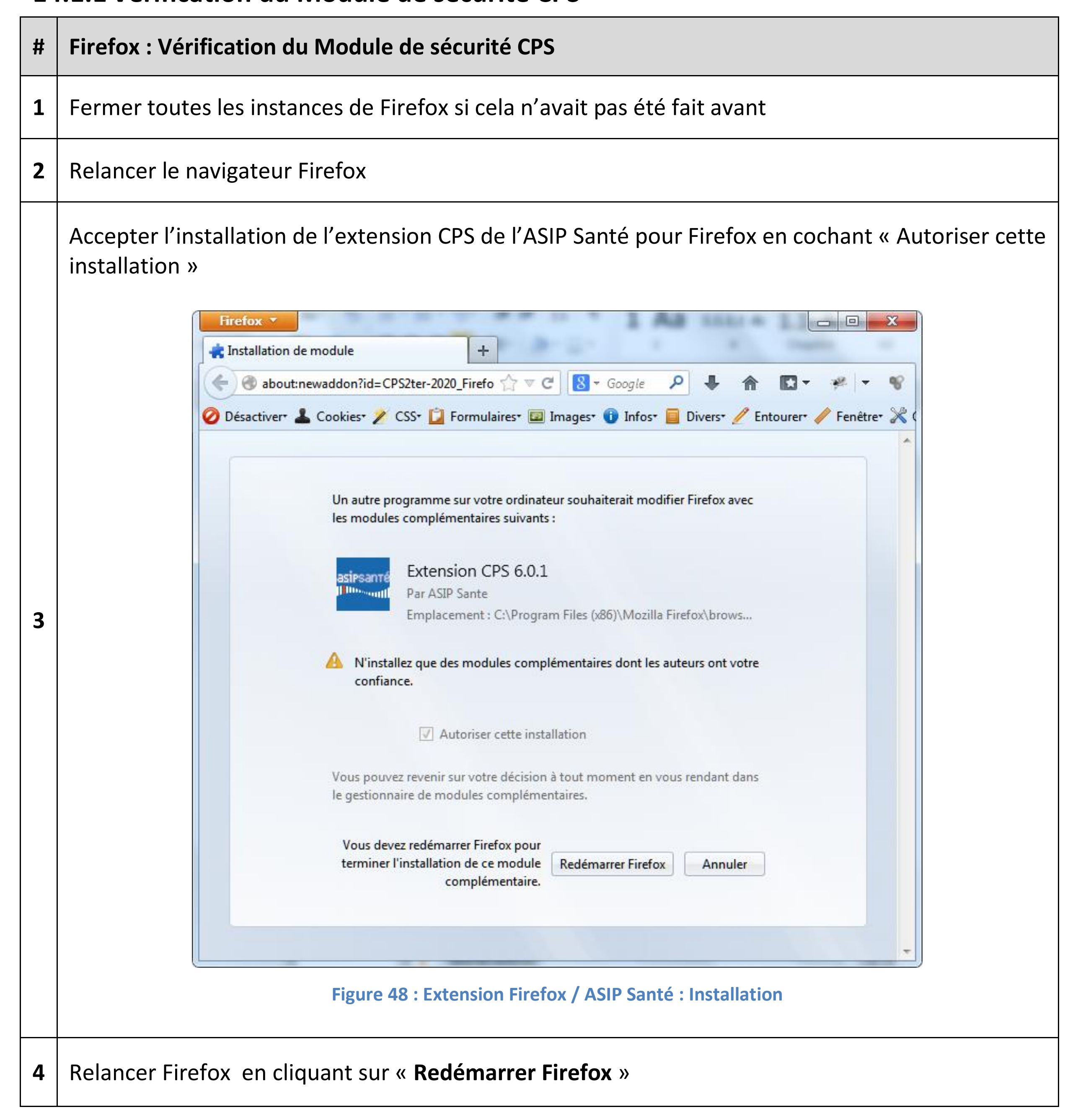
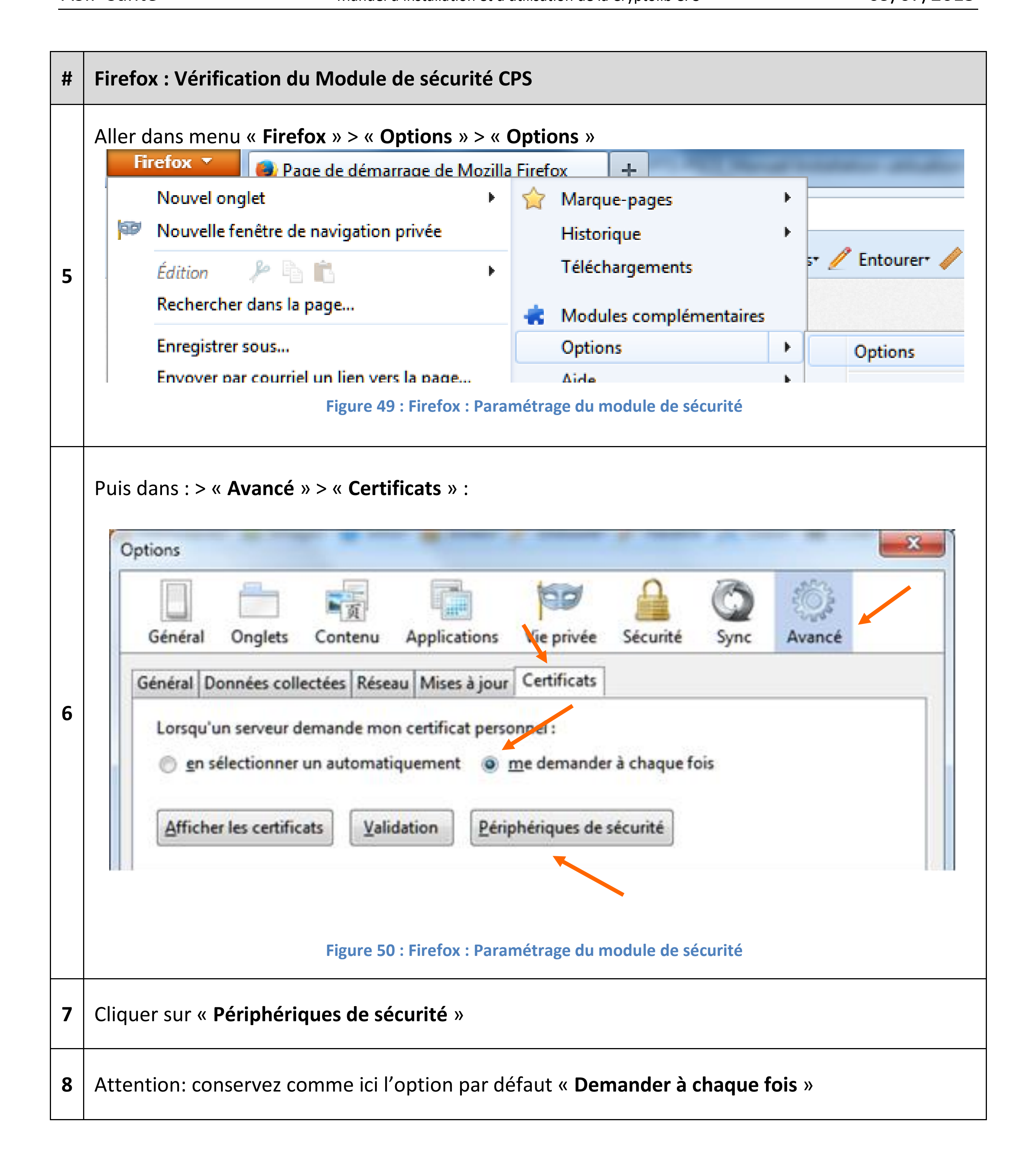


Figure 48 : Extension Firefox / ASIP Santé : Installation</td></tr>
<tr><td>4</td><td>Relancer Firefox en cliquant sur « Redémarrer Firefox »</td></tr>
</table>



#	Firefox : Vérification du Module de sécurité CPS
5	Aller dans menu « **Firefox** » > « **Options** » > « **Options** » Figure 49 : Firefox : Paramétrage du module de sécurité
6	Puis dans : > « **Avancé** » > « **Certificats** » : Figure 50 : Firefox : Paramétrage du module de sécurité
7	Cliquer sur « **Périphériques de sécurité** »
8	Attention: conservez comme ici l'option par défaut « **Demander à chaque fois** »

<table>
<tr><th>#</th><th>Firefox : Vérification du Module de sécurité CPS</th></tr>
<tr><td>9</td><td>

Lorsque la **carte CPx insérée dans le lecteur** est bien **reconnue** et que le **Module de sécurité CPS** est bien installé, la fenêtre suivante apparait :

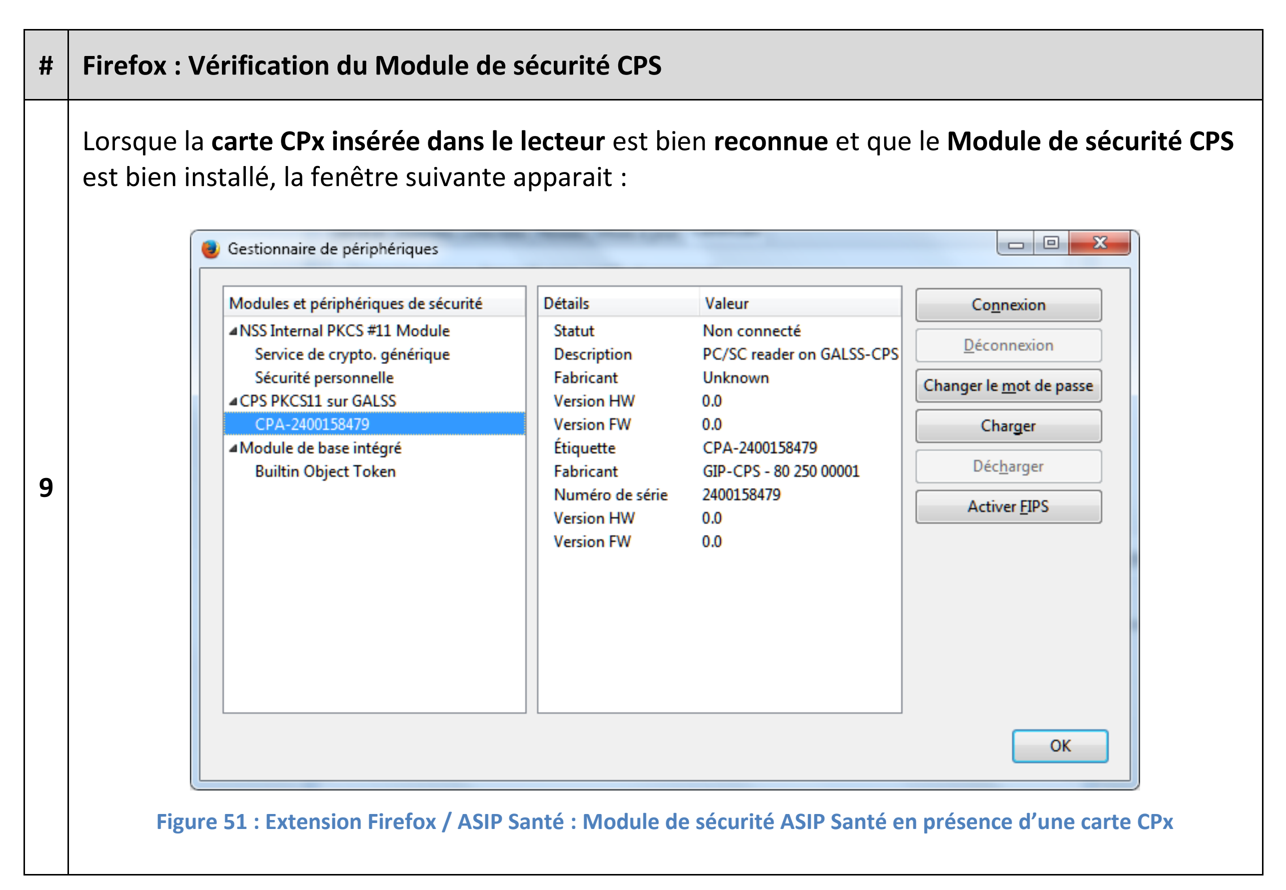


Figure 51 : Extension Firefox / ASIP Santé : Module de sécurité ASIP Santé en présence d’une carte CPx

</td></tr>
</table>

Tableau 48 : Firefox : Vérification du Module de sécurité CPS

14.1.2 Vérification du magasin de certificats Firefox

ID	Contrôle de l'état du Magasin de certificats Firefox	Résultat
MG_01	Insérer une carte CPx dans le lecteur	
MG_02	Lancer Firefox puis aller dans le menu « **Outils** » > « **Options** » : Figure 52 : Firefox : Vérification du magasin de certificat	
MG_03	Puis dans « **Avancé** » > « **Certificats** » > « **Afficher les certificats** » : Figure 53 : Firefox : Vérification du magasin de certificat	
MG_04	La saisie du code porteur de la CPS peut être demandée : Figure 54 : Firefox : Vérification du magasin de certificat Mozilla Firefox n'affiche pas le nombre de tentatives de saisies du code porteur restantes, du fait d'une limitation intrinsèque à Firefox.	

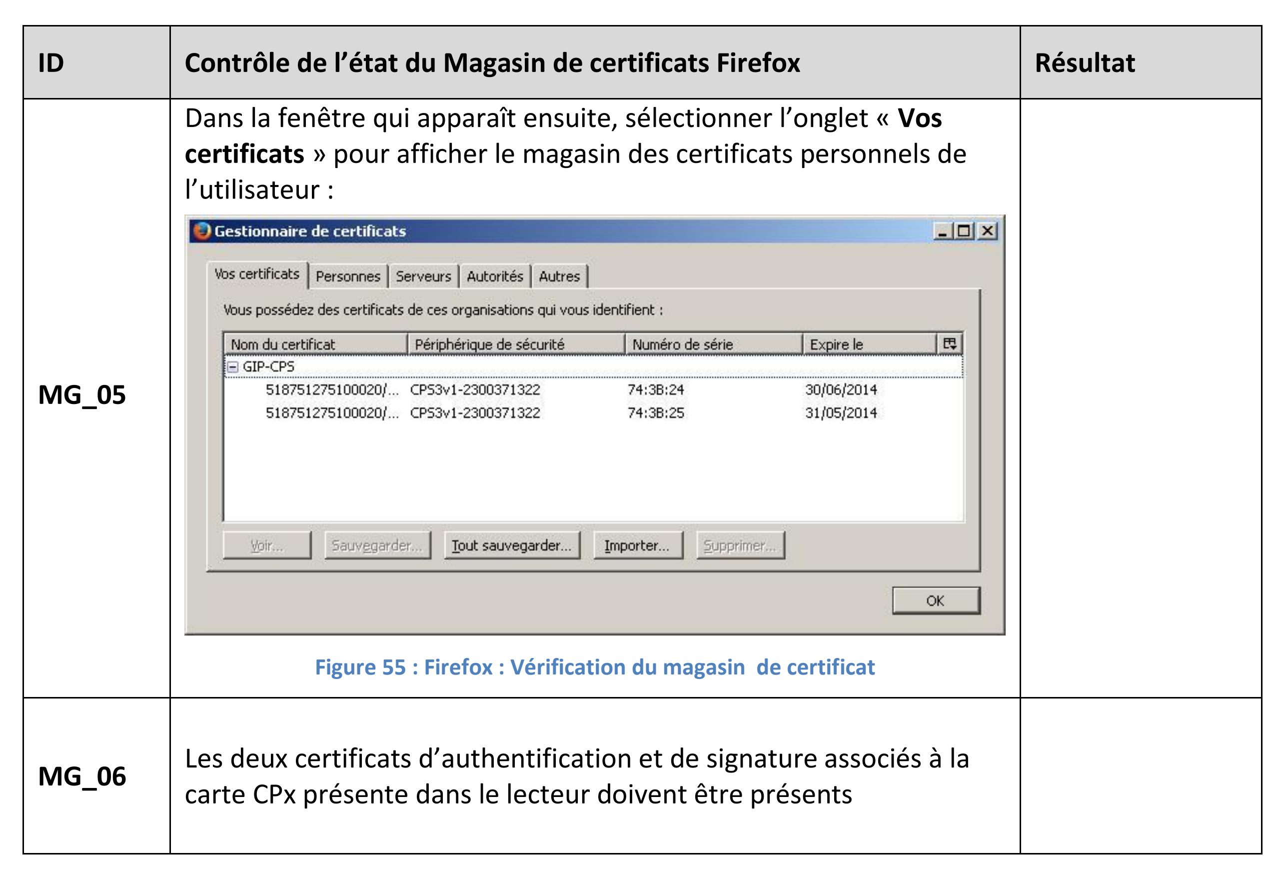
ID	Contrôle de l'état du Magasin de certificats Firefox	Résultat
MG_05	Dans la fenêtre qui apparaît ensuite, sélectionner l'onglet « **Vos certificats** » pour afficher le magasin des certificats personnels de l'utilisateur :  Figure 55 : Firefox : Vérification du magasin de certificat	
MG_06	Les deux certificats d'authentification et de signature associés à la carte CPx présente dans le lecteur doivent être présents	

Tableau 49 : Contrôles : Contrôle de l'état du Magasin Firefox

ID	Contrôle de l'état du Magasin Firefox : Gestion des erreurs	Résultat
MG _81	Vérifier que le lecteur de carte est bien branché	
MG _82	Vérifier que la carte CPx est bien insérée dans le lecteur	
MG _83	Vérifier l'état du GALSS (cf. plus haut)	
MG _84	Vérifier l'installation avec CPS-Gestion (cf. plus haut)	

Tableau 50 : Contrôles : Contrôle de l'état du Magasin Firefox: Gestion des erreurs

14.1.3 Installation du module de sécurité CPS depuis http://testssl.asipsante.fr

Si le module de sécurité CPS pour Firefox n'est pas installé, il est possible de le faire depuis http://testssl.asipsante.fr

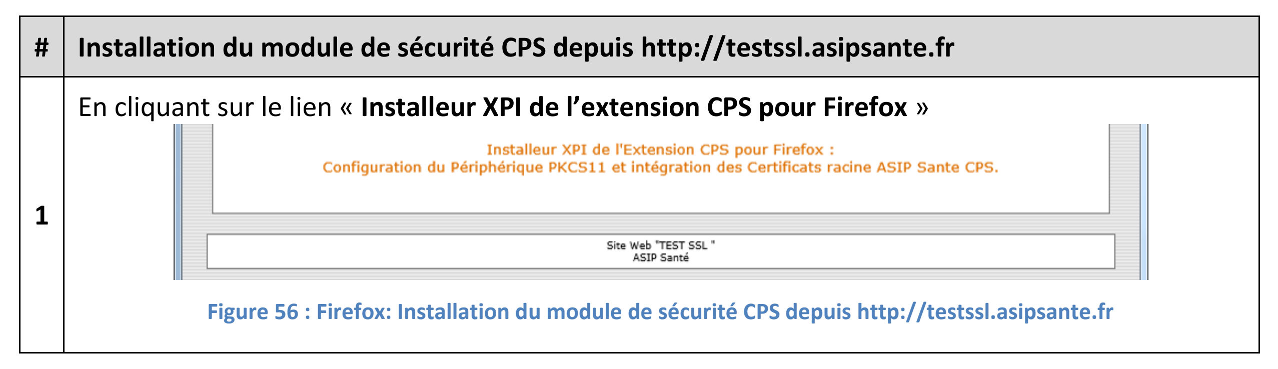
#	Installation du module de sécurité CPS depuis http://testssl.asipsante.fr
1	En cliquant sur le lien « **Installeur XPI de l'extension CPS pour Firefox** »  Figure 56 : Firefox: Installation du module de sécurité CPS depuis http://testssl.asipsante.fr

Tableau 51 : Firefox: Installation du module de sécurité CPS depuis http://testssl.asipsante.fr

14.1.4 Installation manuelle du module de sécurité CPS

Si le module de sécurité CPS pour Firefox n'est pas installé, il est possible de le faire manuellement.

#	Installation manuelle du module de sécurité CPS
1	(voir ci-dessous)

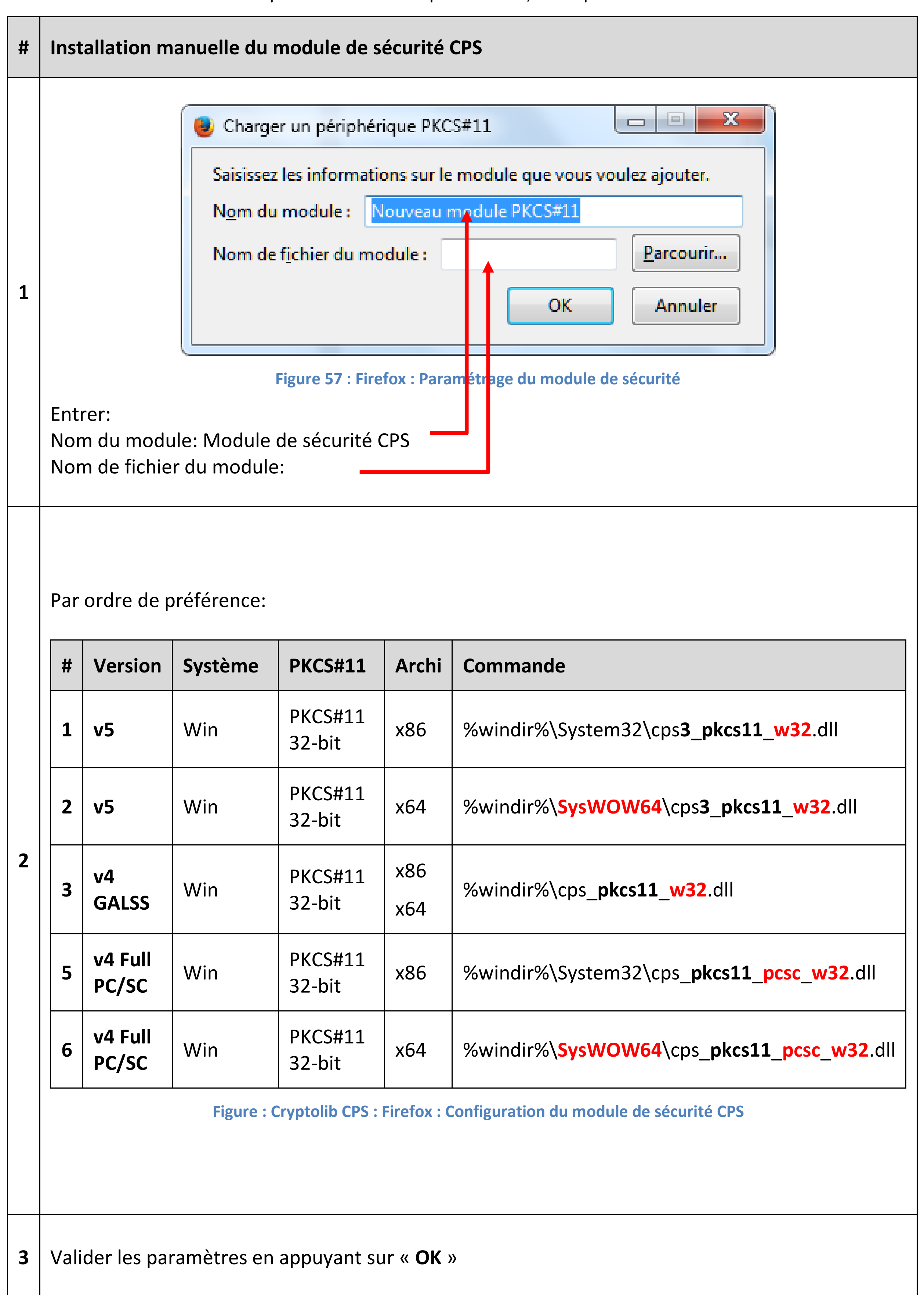


Figure 57 : Firefox : Paramétrage du module de sécurité

Entrer:
Nom du module: Module de sécurité CPS
Nom de fichier du module:

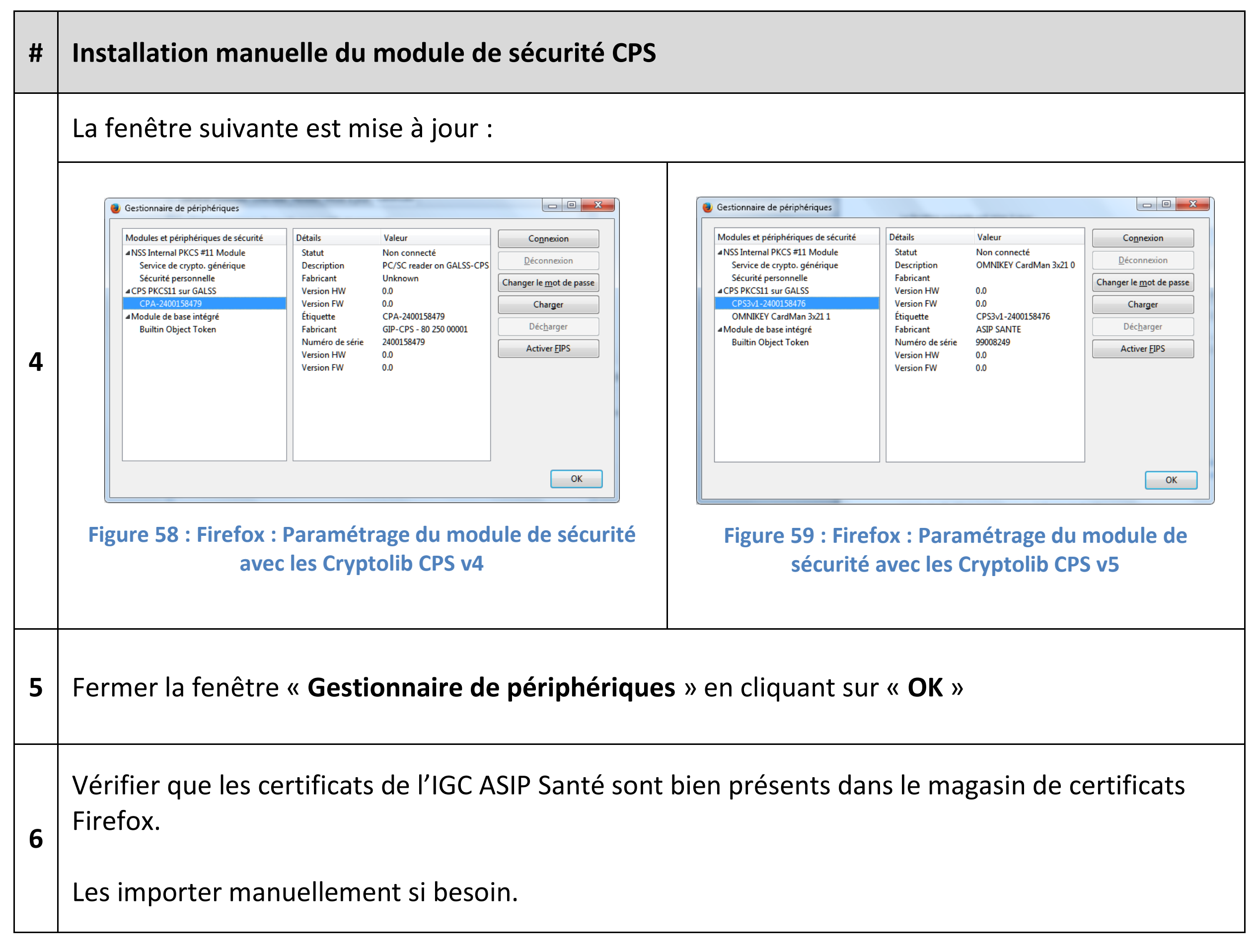
2

Par ordre de préférence:

#	Version	Système	PKCS#11	Archi	Commande
1	**v5**	Win	PKCS#11 32-bit	x86	%windir%\System32\cps**3_pkcs11_w32**.dll
2	**v5**	Win	PKCS#11 32-bit	x64	%windir%**SysWOW64**\cps**3_pkcs11_w32**.dll
3	**v4 GALSS**	Win	PKCS#11 32-bit	x86 x64	%windir%\cps_**pkcs11_w32**.dll
5	**v4 Full PC/SC**	Win	PKCS#11 32-bit	x86	%windir%\System32\cps_**pkcs11_pcsc_w32**.dll
6	**v4 Full PC/SC**	Win	PKCS#11 32-bit	x64	%windir%**SysWOW64**\cps_**pkcs11_pcsc_w32**.dll

Figure : Cryptolib CPS : Firefox : Configuration du module de sécurité CPS

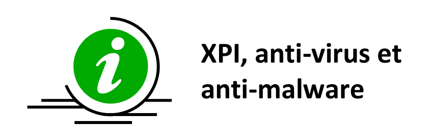
#	
3	Valider les paramètres en appuyant sur « **OK** »



#	Installation manuelle du module de sécurité CPS	
4	La fenêtre suivante est mise à jour :	
	Figure 58 : Firefox : Paramétrage du module de sécurité avec les Cryptolib CPS v4	Figure 59 : Firefox : Paramétrage du module de sécurité avec les Cryptolib CPS v5
5	Fermer la fenêtre « **Gestionnaire de périphériques** » en cliquant sur « **OK** »	
6	Vérifier que les certificats de l'IGC ASIP Santé sont bien présents dans le magasin de certificats Firefox. Les importer manuellement si besoin.	

Tableau 52 : Firefox: Installation manuelle du module de sécurité CPS

La configuration du module de sécurité est terminée : le test de la connexion HTTPS peut être effectué.



XPI, anti-virus et anti-malware

Certains anti-virus et anti-malwares désactive le module de sécurité CPS, ce qui rend inopérante la détection de la carte CPS par Firefox. Dans ce cas, la réinstallation du .XPI ne réactive pas non plus le module : il faut se rendre dans la liste des modules et réactiver le module CPS à la main explicitement.

Tableau 53 : Firefox: Module de sécurité CPS, antivirus et anti-malware

14.1.5 Etat du module

L'état d'activation du module de sécurité CPS peut être aussi vérifié en allant dans « outils > Modules complémentaires » ou en tapant « about:addons » dans la barre d'adresse.

Si le module apparait grisé avec la possibilité de l' « Activer », le module est dans l'état « désactivé » :

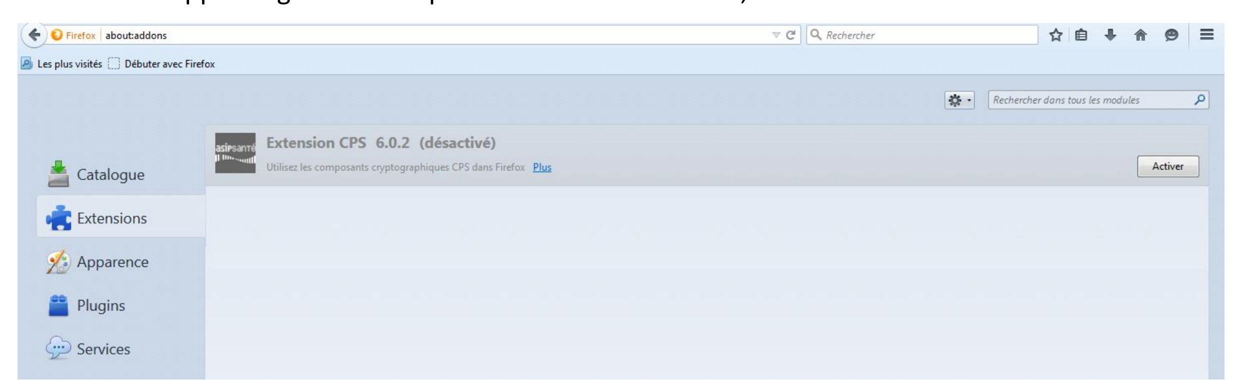


Figure 60 : Module de sécurité CPS désactivé

Il est donc possible de l'activer (nécessaire pour que le carte CPx soit détectée) en cliquant sur « Activer ».

Ce cas de figure peut apparaitre si :

1- La fenêtre d'installation du module de sécurité n'a pas été validée :

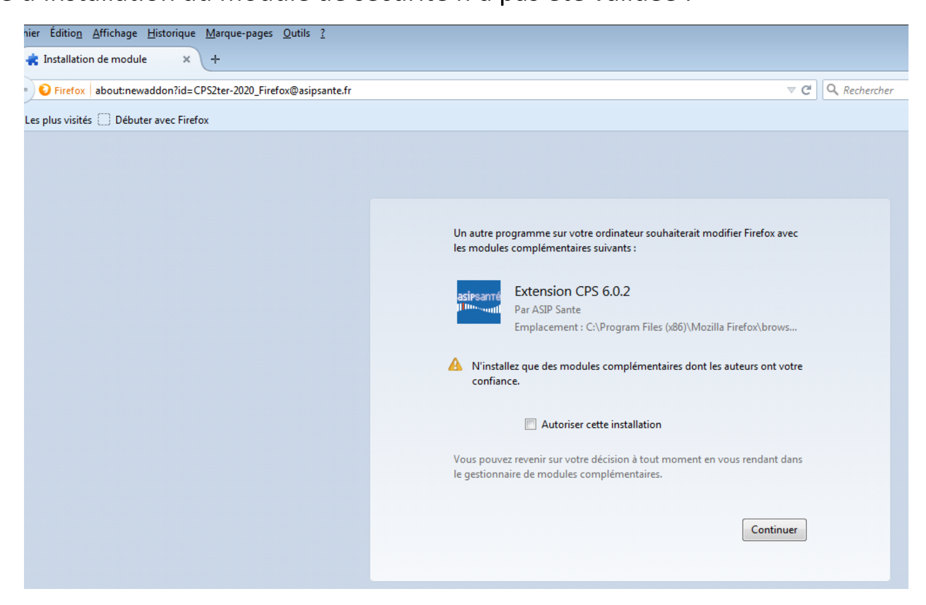
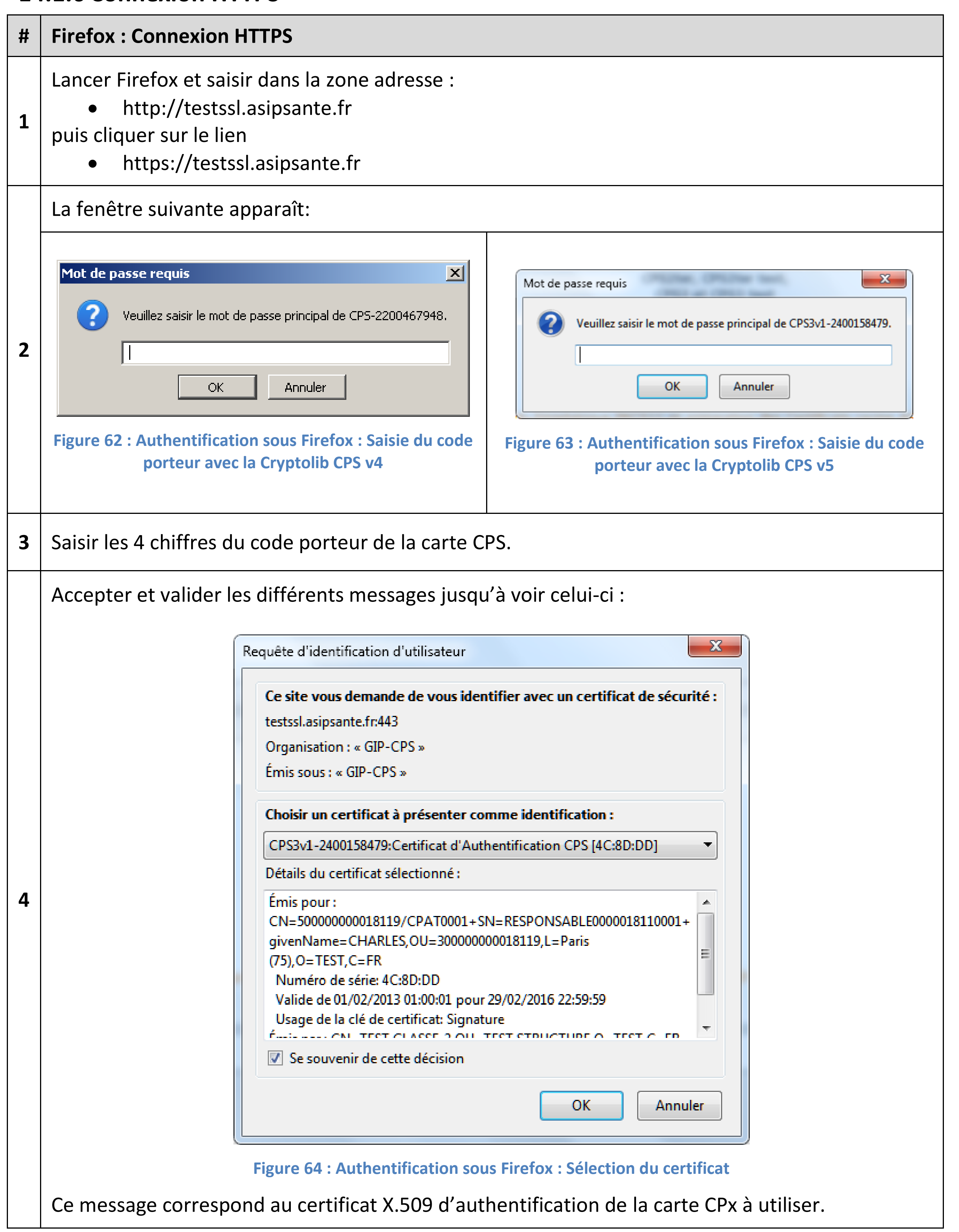


Figure 61 : fenêtre d'installation du module de sécurité

2- Un antivirus ou un anti-spyware a été exécuté sur la machine et a pu désactiver le module.

14.1.6 Connexion HTTPS



#	Firefox : Connexion HTTPS
1	Lancer Firefox et saisir dans la zone adresse : • http://testssl.asipsante.fr puis cliquer sur le lien • https://testssl.asipsante.fr
2	La fenêtre suivante apparaît: Figure 62 : Authentification sous Firefox : Saisie du code porteur avec la Cryptolib CPS v4 Figure 63 : Authentification sous Firefox : Saisie du code porteur avec la Cryptolib CPS v5
3	Saisir les 4 chiffres du code porteur de la carte CPS.
4	Accepter et valider les différents messages jusqu'à voir celui-ci : Figure 64 : Authentification sous Firefox : Sélection du certificat Ce message correspond au certificat X.509 d'authentification de la carte CPx à utiliser.

#	Firefox : Connexion HTTPS
5	En cas de succès de l'authentification, la page suivante apparaît:

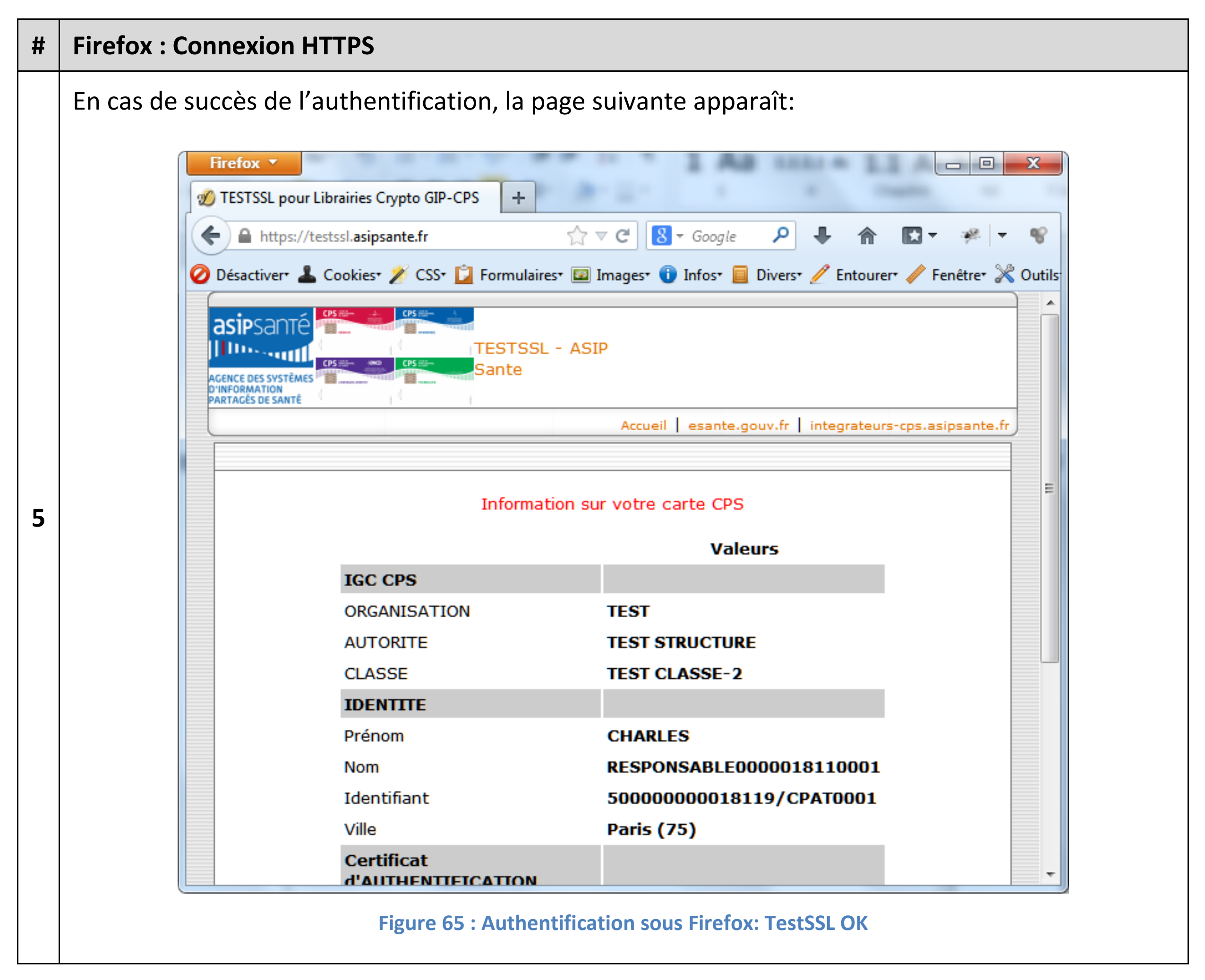


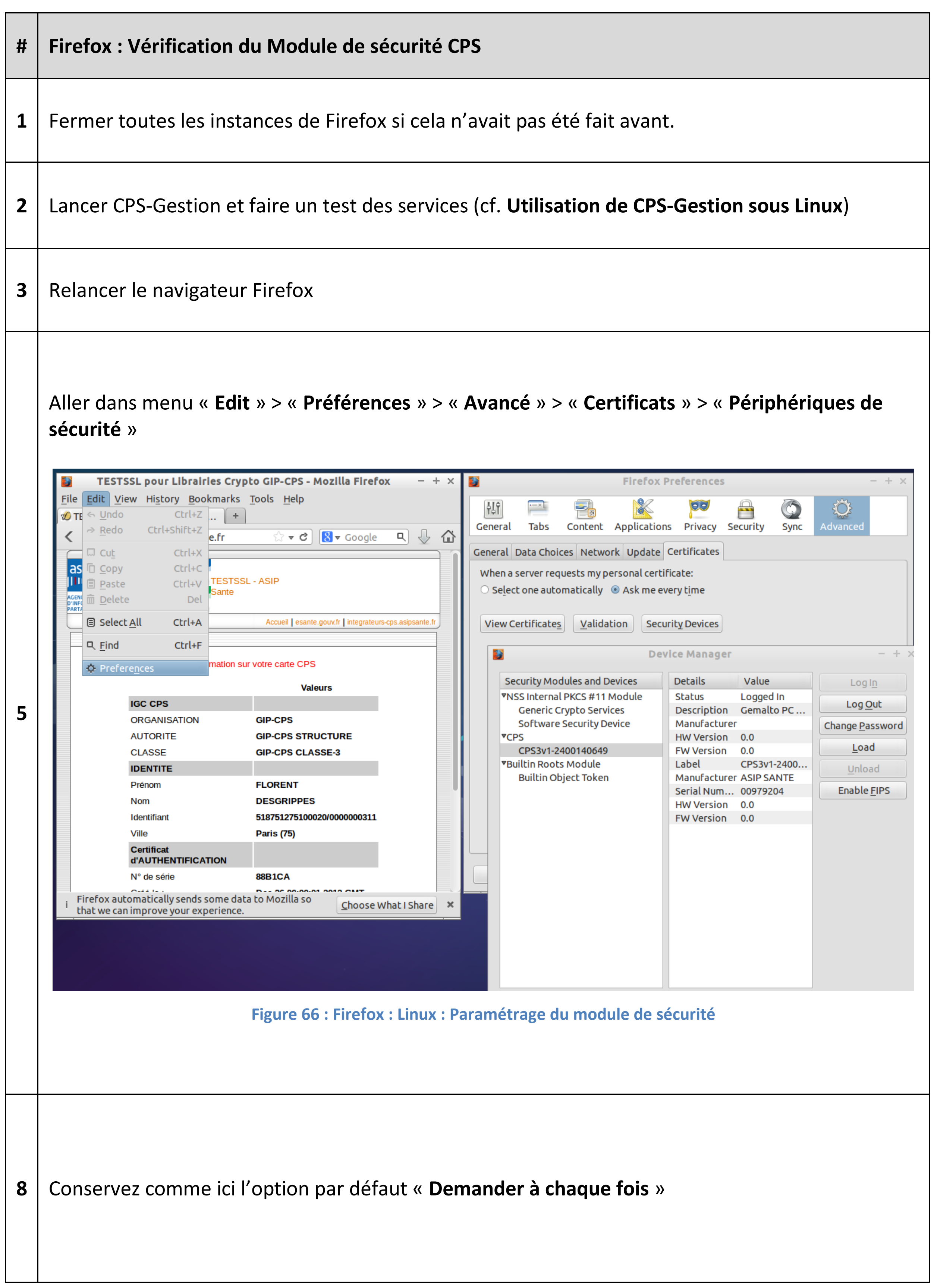
Figure 65 : Authentification sous Firefox: TestSSL OK

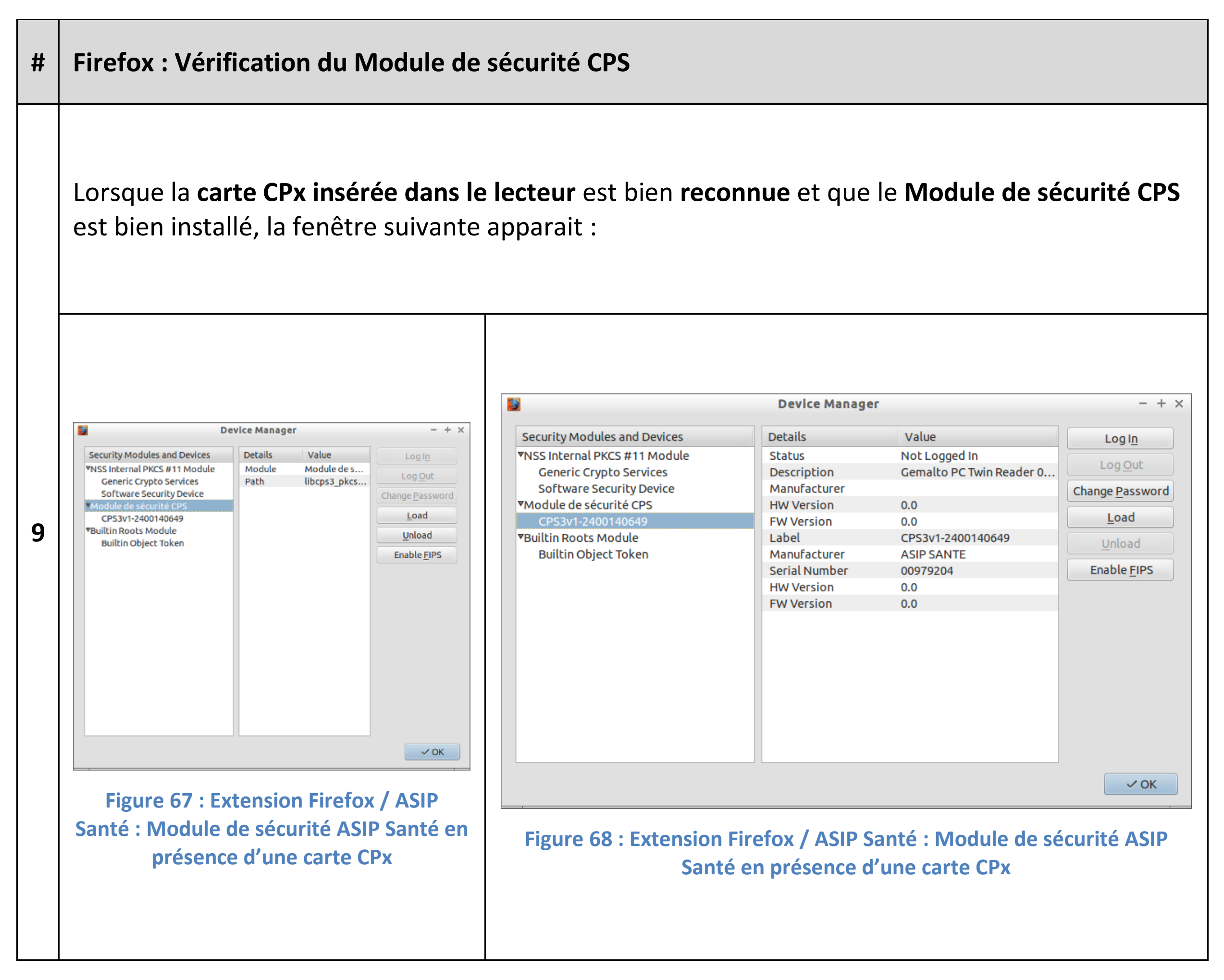
Tableau 54 : Firefox : Connexion HTTPS

L'apparition de cette page garantit que l'installation des composants logiciels s'est déroulée correctement.

14.2 Utilisations avec Firefox sous Linux

14.2.1 Vérification du Module de sécurité CPS

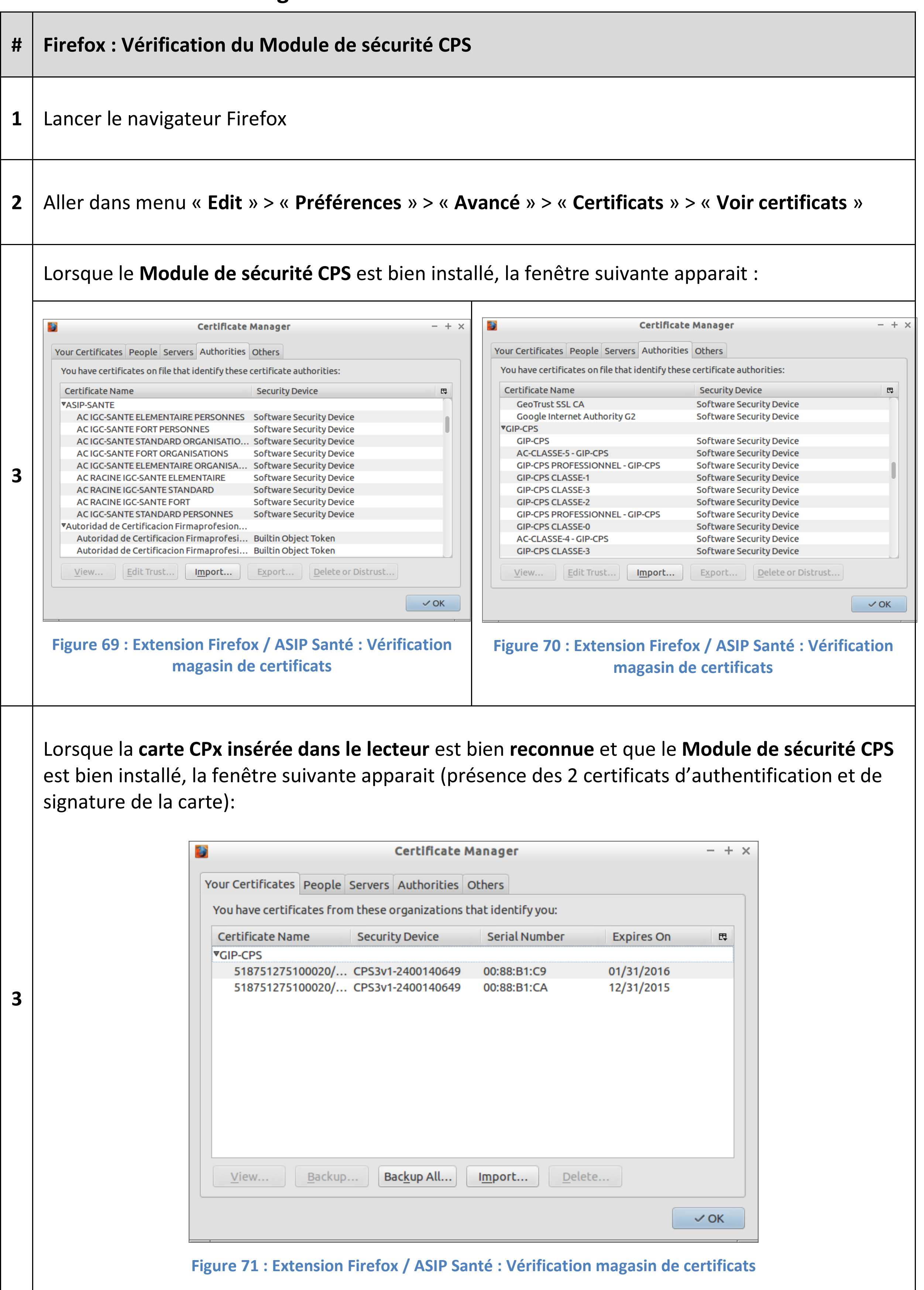
#	Firefox : Vérification du Module de sécurité CPS
1	Fermer toutes les instances de Firefox si cela n'avait pas été fait avant.
2	Lancer CPS-Gestion et faire un test des services (cf. **Utilisation de CPS-Gestion sous Linux**)
3	Relancer le navigateur Firefox
5	Aller dans menu « **Edit** » > « **Préférences** » > « **Avancé** » > « **Certificats** » > « **Périphériques de sécurité** »  Figure 66 : Firefox : Linux : Paramétrage du module de sécurité
8	Conservez comme ici l'option par défaut « **Demander à chaque fois** »



#	Firefox : Vérification du Module de sécurité CPS	
9	Lorsque la **carte CPx insérée dans le lecteur** est bien **reconnue** et que le **Module de sécurité CPS** est bien installé, la fenêtre suivante apparait :	
	Figure 67 : Extension Firefox / ASIP Santé : Module de sécurité ASIP Santé en présence d'une carte CPx	Figure 68 : Extension Firefox / ASIP Santé : Module de sécurité ASIP Santé en présence d'une carte CPx

Tableau 55 : Firefox : Linux : Vérification du Module de sécurité CPS

14.2.2 Vérification du magasin de certificats Firefox



#	Firefox : Vérification du Module de sécurité CPS
1	Lancer le navigateur Firefox
2	Aller dans menu « **Edit** » > « **Préférences** » > « **Avancé** » > « **Certificats** » > « **Voir certificats** »
3	Lorsque le **Module de sécurité CPS** est bien installé, la fenêtre suivante apparait : Figure 69 : Extension Firefox / ASIP Santé : Vérification magasin de certificats Figure 70 : Extension Firefox / ASIP Santé : Vérification magasin de certificats
3	Lorsque la **carte CPx insérée dans le lecteur** est bien **reconnue** et que le **Module de sécurité CPS** est bien installé, la fenêtre suivante apparait (présence des 2 certificats d'authentification et de signature de la carte): Figure 71 : Extension Firefox / ASIP Santé : Vérification magasin de certificats

Tableau 56 : Firefox : Linux : Vérification du magasin de certificats

14.2.3 Installation du module de sécurité CPS depuis http://testssl.asipsante.fr

Si le module de sécurité CPS pour Firefox n'est pas installé, il est possible de le faire depuis http://testssl.asipsante.fr

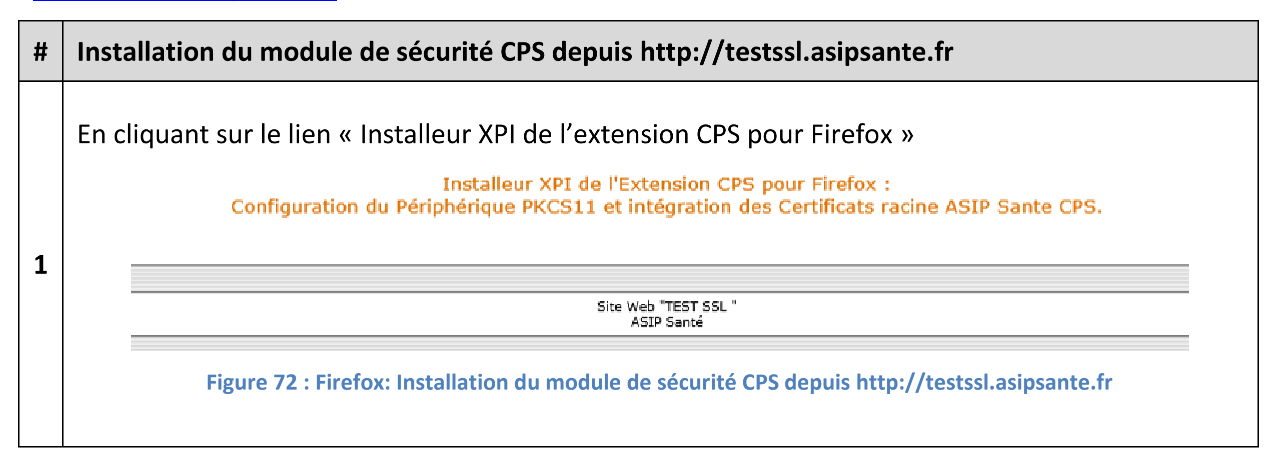
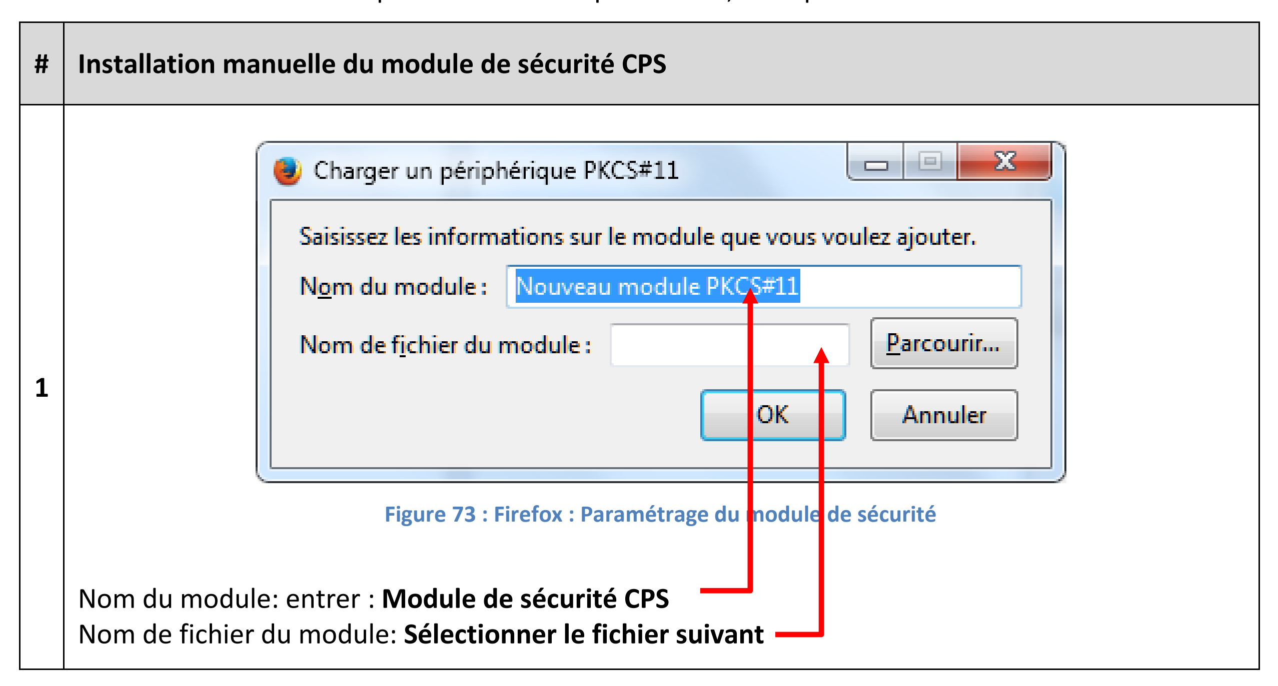
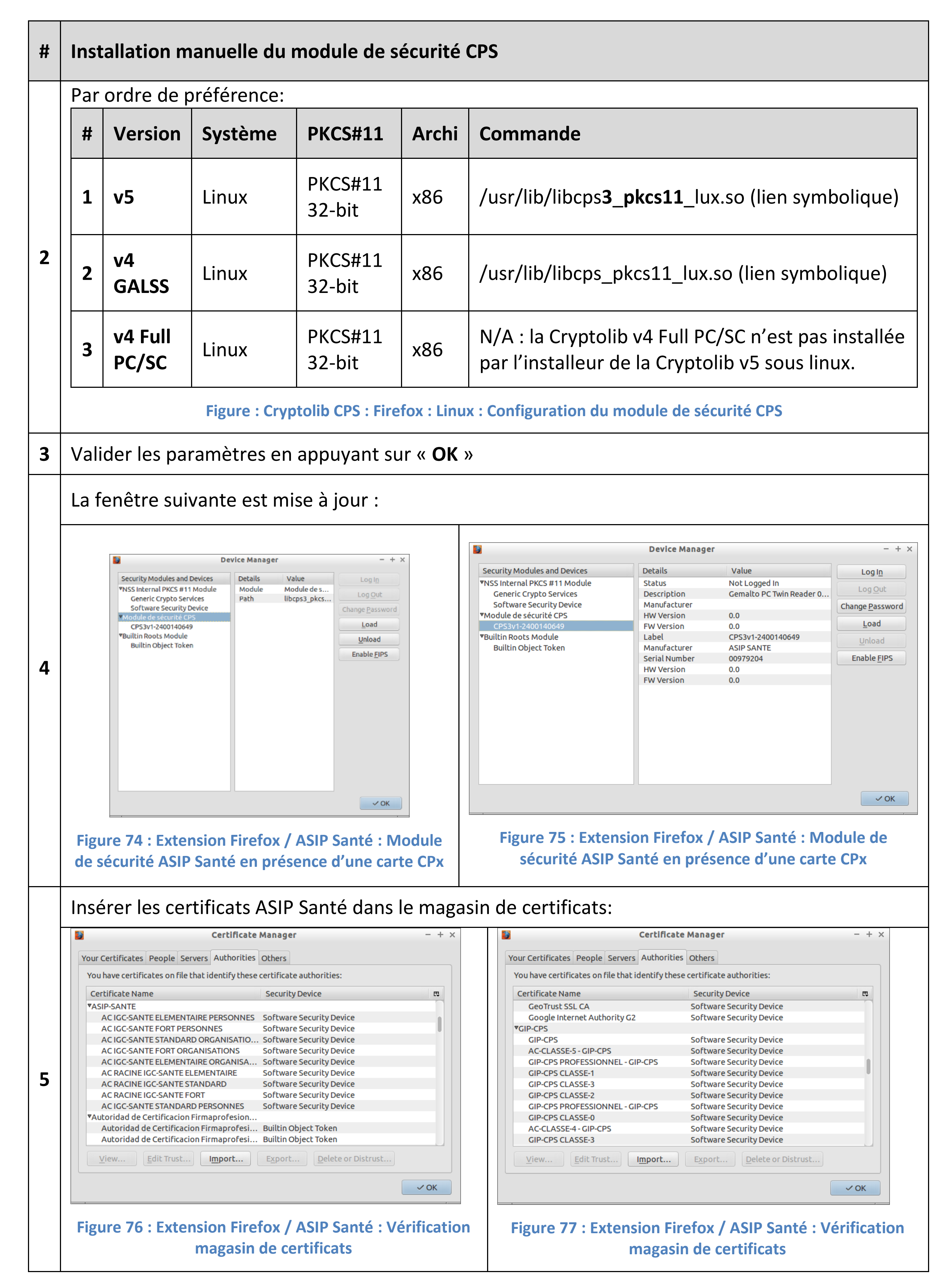
#	Installation du module de sécurité CPS depuis http://testssl.asipsante.fr
1	En cliquant sur le lien « Installeur XPI de l'extension CPS pour Firefox »  Figure 72 : Firefox: Installation du module de sécurité CPS depuis http://testssl.asipsante.fr

Tableau 57 : Firefox: Installation du module de sécurité CPS depuis http://testssl.asipsante.fr

14.2.4 Installation manuelle du module de sécurité CPS

Si le module de sécurité CPS pour Firefox n'est pas installé, il est possible de le faire manuellement.

#	Installation manuelle du module de sécurité CPS
1	 Figure 73 : Firefox : Paramétrage du module de sécurité Nom du module: entrer : **Module de sécurité CPS** Nom de fichier du module: **Sélectionner le fichier suivant**



#	Installation manuelle du module de sécurité CPS
2	Par ordre de préférence:

#	Version	Système	PKCS#11	Archi	Commande
1	**v5**	Linux	PKCS#11 32-bit	x86	/usr/lib/libcps**3_pkcs11**_lux.so (lien symbolique)
2	**v4 GALSS**	Linux	PKCS#11 32-bit	x86	/usr/lib/libcps_pkcs11_lux.so (lien symbolique)
3	**v4 Full PC/SC**	Linux	PKCS#11 32-bit	x86	N/A : la Cryptolib v4 Full PC/SC n'est pas installée par l'installeur de la Cryptolib v5 sous linux.

Figure : Cryptolib CPS : Firefox : Linux : Configuration du module de sécurité CPS

#	
3	Valider les paramètres en appuyant sur « **OK** »
4	La fenêtre suivante est mise à jour :

Figure 74 : Extension Firefox / ASIP Santé : Module de sécurité ASIP Santé en présence d'une carte CPx

Figure 75 : Extension Firefox / ASIP Santé : Module de sécurité ASIP Santé en présence d'une carte CPx

#	
5	Insérer les certificats ASIP Santé dans le magasin de certificats:

Figure 76 : Extension Firefox / ASIP Santé : Vérification magasin de certificats

Figure 77 : Extension Firefox / ASIP Santé : Vérification magasin de certificats

Tableau 58 : Firefox: Installation manuelle du module de sécurité CPS

Une fois la configuration du module de sécurité terminée, le test de la connexion HTTPS peut être effectué.

14.2.5 Etat du module

Idem que sous Microsoft Windows.

14.2.6 Connexion HTTPS

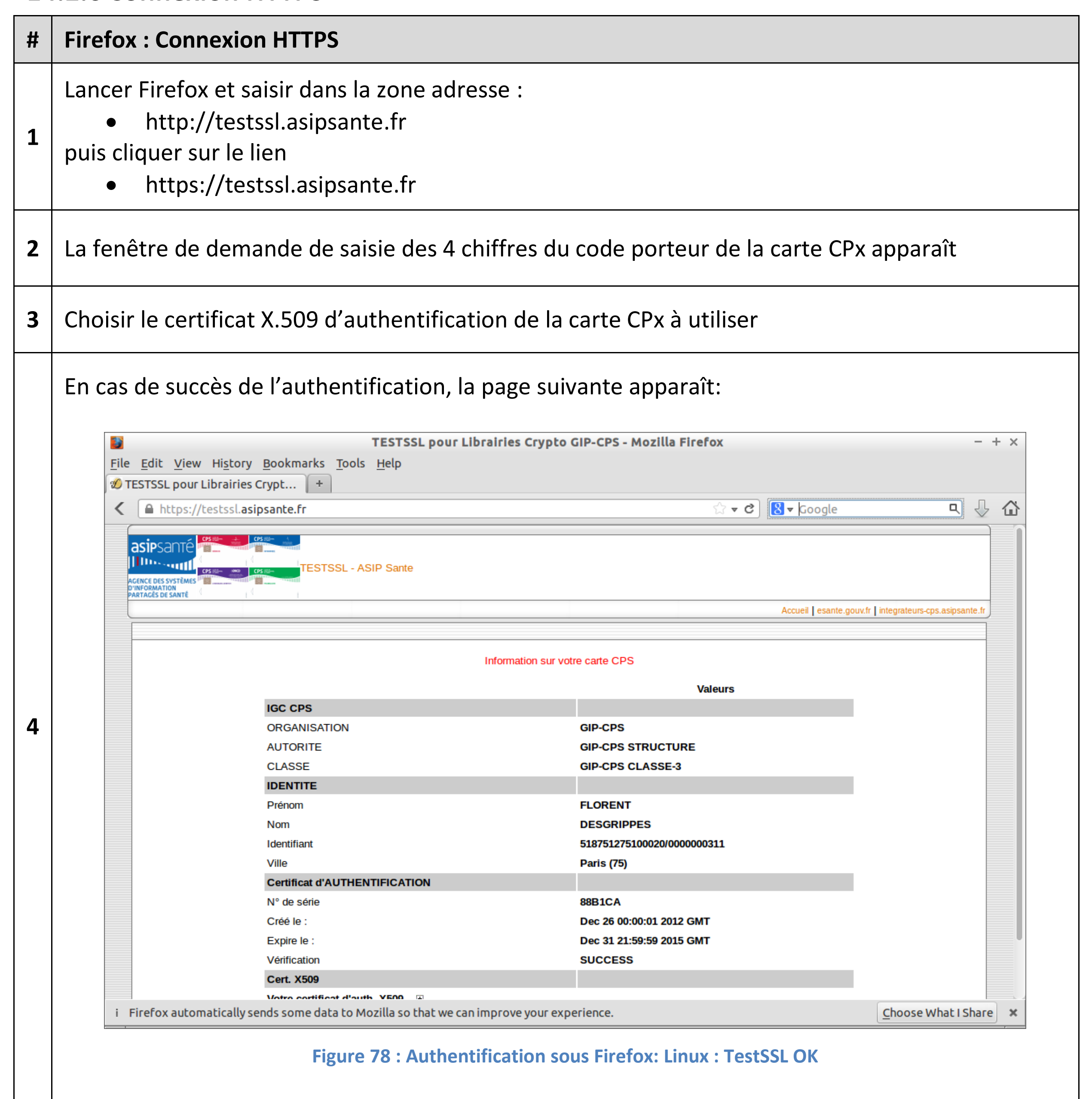
#	Firefox : Connexion HTTPS
1	Lancer Firefox et saisir dans la zone adresse : • http://testssl.asipsante.fr puis cliquer sur le lien • https://testssl.asipsante.fr
2	La fenêtre de demande de saisie des 4 chiffres du code porteur de la carte CPx apparaît
3	Choisir le certificat X.509 d'authentification de la carte CPx à utiliser
4	En cas de succès de l'authentification, la page suivante apparaît:  Figure 78 : Authentification sous Firefox: Linux : TestSSL OK

Tableau 59 : Firefox : Linux : Connexion HTTPS

L'apparition de cette page garantit que l'installation des composants logiciels s'est déroulée correctement.



15Installations et utilisations avancées

15.1 Contrôles des fichiers logiciels installés

Le tableau suivant résume l'emplacement des différents composants sur le poste. Les Release Notes restent la référence pour ce type d'information.

Module	Composant	Windows		Linux		Mac OS X	
GALSS[12] = gestionnaire d'accès aux lecteurs	Gestion Client Information Poste GALSS Protocole PCSC Protocole PSS	%WINDIR%	galclw32.dll galinw32.dll galssw32.dll pcscw32.dll pssinw32.dll	/usr/local/galss	libgalcllux.so libgalinlux.so libgalsslux.so libpcsclux.so libpssinlux.so	/Library/Frameworks	galclosx.framework galinosx.framework galssosx.framework pcscosx.framework pssinosx.framework
	Configuration	%WINDIR%	galss.ini	/usr/local/galss	galss.ini io_comm.ini	/Library/Preferences	galss.ini io_comm.ini
	Gestion Serveur	%WINDIR%	galsvw32.exe	/usr/local/galss	galsvlux	/Library/Application Support/Galss	galsvosx

[12] Remarque : sur un poste déjà équipé d'un lecteur et d'une solution de FSE, le setup Cryptolib CPS par défaut ne modifie pas la couche GALSS. Seules les couches API-CPS et Cryptolib CPS sont mises à jour dans ce cas. Pour forcer la mise à jour du composant GALSS, supprimez ou renommez le fichier galss.ini existant avant de lancer l'installation.

Module	Composant	Windows		Linux		Mac OS X	
API-CPS = Services de la CPx	Gestion Carte CPS Gestion Dictionnaire	%WINDIR%	cpsw32.dll cptabw32.dll sscasw32.dll	/usr/local/galss	libcpslux.so libcptablux.so libsscaslux.so	/Library/Frameworks	cpsosx.framework cptabosx.framework sscasosx.framework
	Dictionnaire	%WINDIR%	DICO-FR.GIP	/etc/opt/santesocial/CPS/	DICO-FR.GIP	/Library/Preferences	DICO-FR.GIP
Application de Gestion de la CPx	CPS-Gestion	%WINDIR%		/usr/bin	cpgeslux	/Applications	cpgesosx iocomcnf
		%ProgramFiles%\santesocial\CPS\ %ProgramFiles(x86)%\santesocial\CPS\	cpgesw32.exe cpgesw64.exe				
Cryptolib CPS	PKCS#11-CPS	%WINDIR%	cps_pkcs11_w32.dll	/usr/local/galss	libcps_pkcs11_lux.so	/usr/lib	libcps_pkcs11_osx.dylib
		%WINSYS%	cps3_pkcs11_w32.dll cps3_pkcs11_w64.dll				
	Configuration	%WINDIR%	cps_pkcs11_safe.ini	/CryptolibCPS	cps_pkcs11_safe.ini	/Library/Preferences	cps_pkcs11_safe.ini
	CSP-CPS	%WINSYS%	cps_csp_w32.dll cps_csp_w32.sig cps3_csp_w32.dll cps3_csp_w64.dll				
	Extensions	%ProgramFiles%\santesocial\CPS\ %ProgramFiles(x86)%\santesocial\CPS\	CCM.exe				
	Tokend CDSA					/System/Library /Security/tokend	GIP-CPS.tokend
Drivers	Driver PC/SC sur lecteur PSS	Gestionnaire de périphériques		dmesg /etc/tty*		/usr/libexec /SmartCardServices /driver	GALSSdriver.bundle
	Configuration du driver	Gestionnaire de périphériques		/usr/local/galss	io_comm.ini Galss.ini	/private/etc	reader.conf[13]

Tableau 60 : Vérification des ressources installées

[13] La présence de ce fichier reader.conf dans /private/etc est indispensable pour une utilisation du navigateur Safari avec des lecteurs bi-fentes PSS. Ce fichier doit en revanche être renommé en reader.gip ou supprimé pour une utilisation avec des lecteurs PC/SC. Une utilisation avec une configuration de lecteurs mixte PSS+PC/SC est à proscrire.



15.2 Installations et utilisations avancées sous Microsoft Windows

15.2.1 Utilisation avancée de la technologie MSI

Se reporter à **[9]** Command-Line Switches for the Microsoft Windows Installer Tool

Les fichiers .MSI peuvent s'installer en ligne de commande.

Ceci s'avère très utile pour obtenir des traces de l'installation, ou effectuer des installations :

1. « **unattended** »
    a. sans intervention de l'utilisateur
        i. en particulier : pas de clic ou de saisie
    b. mais avec une restitution graphique possible
        i. par ex.: état d'avancement
2. « **silent** »
    a. sans aucune saisie utilisateur
    b. sans aucune restitution graphique à l'utilisateur

La ligne de commande d'installation préconisée est la suivante :

```
[start /wait] msiexec [/l*v %PATH_TO_LOG%\[module_name]\msiexec-install.txt] /i msi_name [/qn]
```

Figure : MSI : Ligne de commande préconisée

Explication des paramètres de la ligne de commande d'installation MSIEXEC préconisée		
[start /wait]	facultatif	Démarrer une commande et attend qu'elle finisse (mode synchrone). Particulièrement utile pour enchainer les commandes d'installation MSI.
msiexec	obligatoire	Exécutable « Microsoft Windows Installer »
[/l*v %PATH_TO_LOG%\[module_name]\msiexec-install.txt]	facultatif	Logs de l'installation (chemin complet)
/i msi_name	obligatoire	Nom du fichier .MSI à installer
[/qn]	facultatif	Mode "silent"

Tableau 61 : MSI : Détails des paramètres de la ligne de commande d'installation MSIEXEC préconisée

15.2.2 Répertoire temporaire d'installation

La procédure d'installation utilise un dossier dans lequel elle peut copier les fichiers à sauvegarder et les fichiers temporaires.

L'installation affecte la valeur du chemin complet de ce dossier à la variable %SUPPORTDIR%.

La variable %SUPPORTDIR% est créée à partir de la variable d'environnement %TMP% et du GUID de l'installation (%TMP%\{4748C15E-92F4-4FE8-BB47-6234D0CAE49B} par exemple).

La valeur de %TMP% par défaut est:

C:\DOCUME~1\<USERNA~1>\LOCALS~1\Temp\

La valeur de % SUPPORTDIR % par défaut est :

C:\DOCUME~1\<USERNA~1>\LOCALS~1\Temp\{4748C15E-92F4-4FE8-BB47-6234D0CAE49B}

Important	La valeur de %TMP% doit être spécifiée au format 8.3 sous peine d'erreur à l'installation.

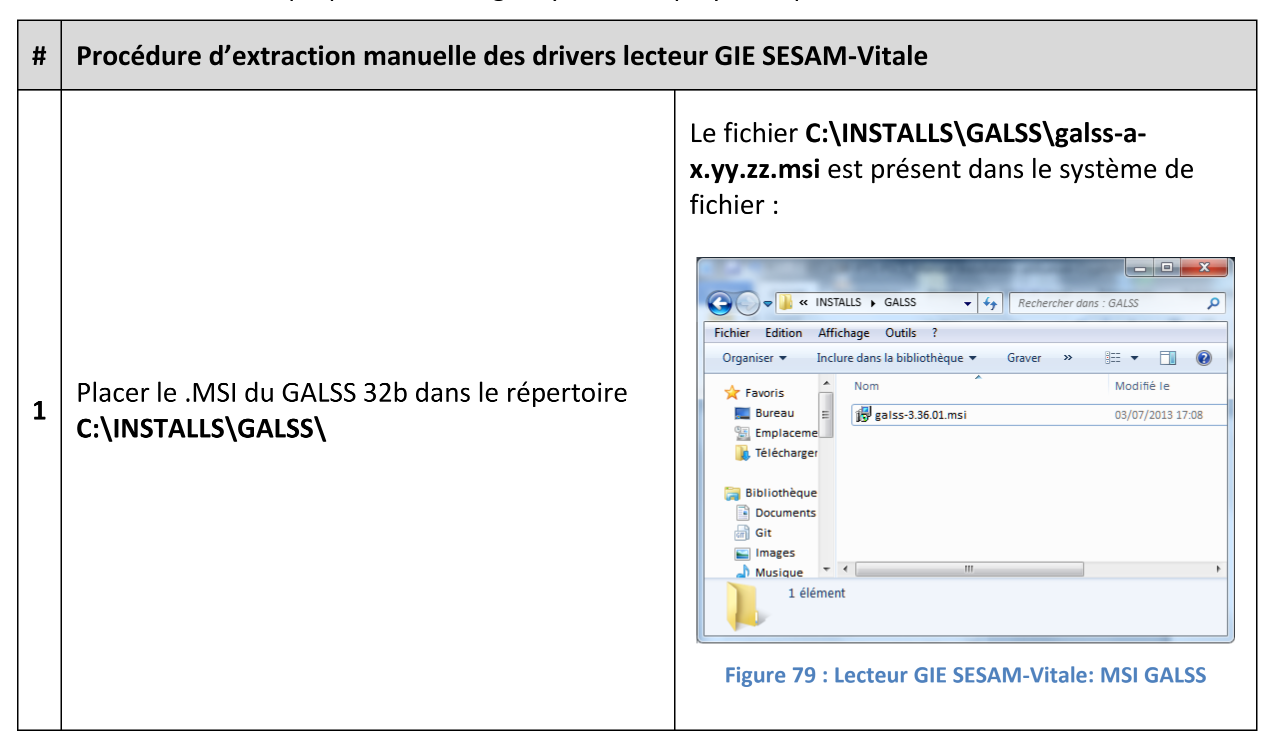
Par exemple : C:\Documents and settings\<Forname Surname>\Local Settings\Temp\ n'est sont pas des chemins valables pour %TMP%.

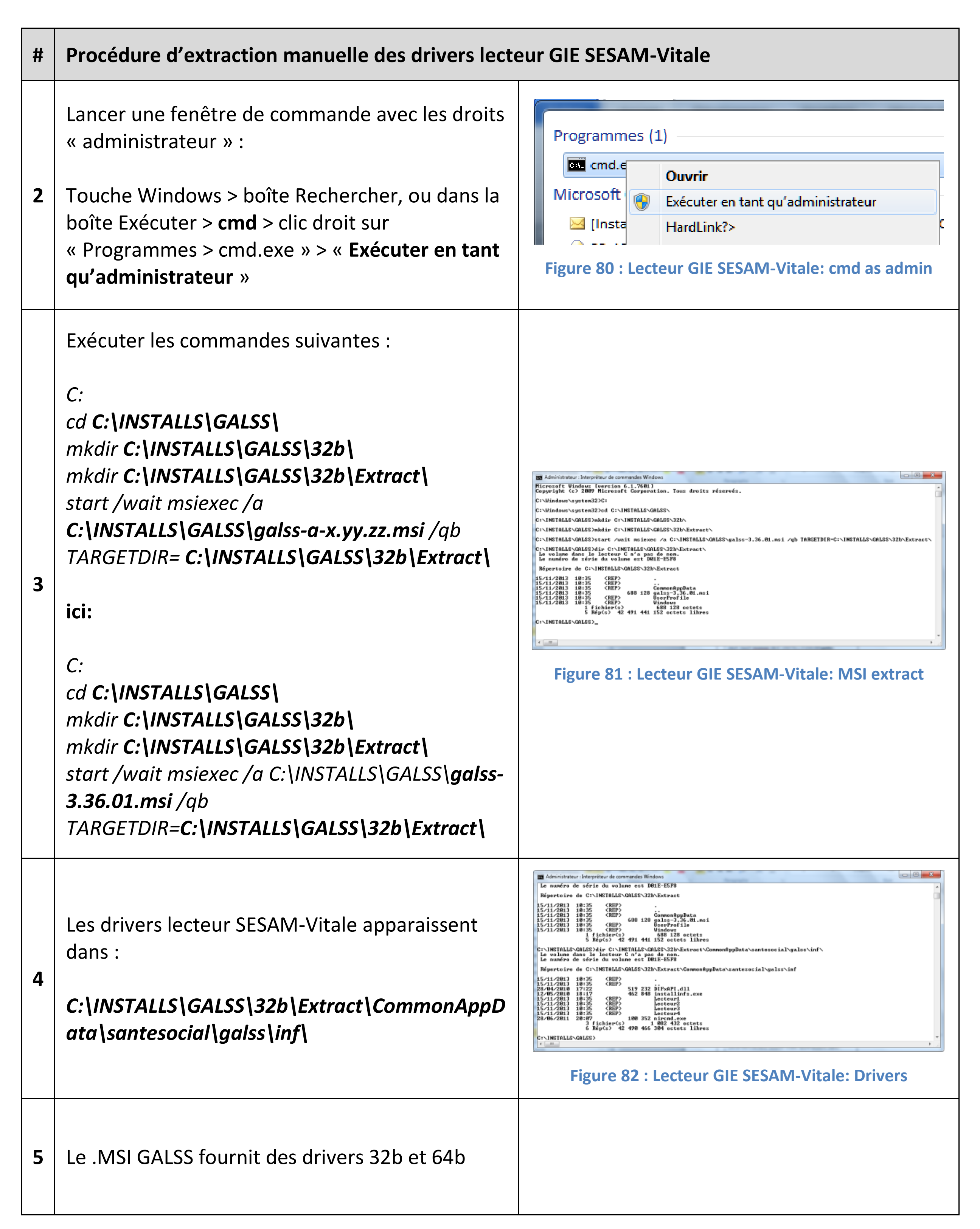
15.2.3 Gestion avancée des drivers lecteur GIE SESAM-Vitale

15.2.3.1 *Extraction des drivers*

Cette procédure est non-intrusive, contrairement à la procédure classique d'installation des drivers lecteur SESAM-Vitale qui consiste à lancer le .MSI du GALSS.

Elle permet aux intégrateurs ou aux établissements d'extraire les drivers lecteur fournis par le GIE SESAM-Vitale afin de préparer des images système déployables provisionnées avec ces drivers.

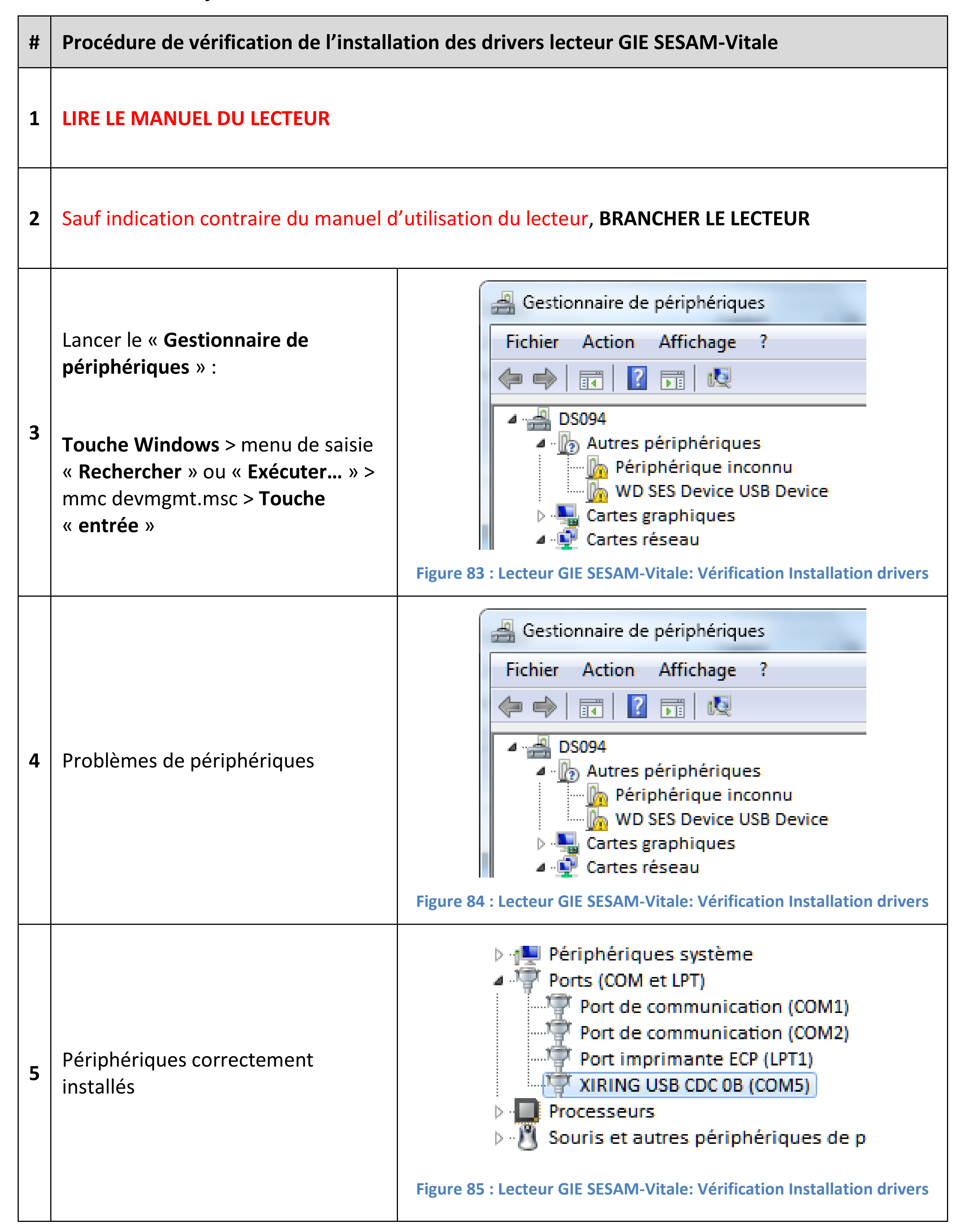
#	Procédure d'extraction manuelle des drivers lecteur GIE SESAM-Vitale	
1	Placer le .MSI du GALSS 32b dans le répertoire **C:\INSTALLS\GALSS**	Le fichier **C:\INSTALLS\GALSS\galss-a-x.yy.zz.msi** est présent dans le système de fichier :  Figure 79 : Lecteur GIE SESAM-Vitale: MSI GALSS



#	Procédure d'extraction manuelle des drivers lecteur GIE SESAM-Vitale	
2	Lancer une fenêtre de commande avec les droits « administrateur » : Touche Windows > boîte Rechercher, ou dans la boîte Exécuter > **cmd** > clic droit sur « Programmes > cmd.exe » > « **Exécuter en tant qu'administrateur** »	Figure 80 : Lecteur GIE SESAM-Vitale: cmd as admin
3	Exécuter les commandes suivantes : *C:* *cd* ***C:\INSTALLS\GALSS*** *mkdir* ***C:\INSTALLS\GALSS\32b*** *mkdir* ***C:\INSTALLS\GALSS\32b\Extract*** *start /wait msiexec /a* ***C:\INSTALLS\GALSS\galss-a-x.yy.zz.msi*** */qb TARGETDIR=* ***C:\INSTALLS\GALSS\32b\Extract*** **ici:** *C:* *cd* ***C:\INSTALLS\GALSS*** *mkdir* ***C:\INSTALLS\GALSS\32b*** *mkdir* ***C:\INSTALLS\GALSS\32b\Extract*** *start /wait msiexec /a C:\INSTALLS\GALSS****galss-3.36.01.msi*** */qb TARGETDIR=****C:\INSTALLS\GALSS\32b\Extract***	Figure 81 : Lecteur GIE SESAM-Vitale: MSI extract
4	Les drivers lecteur SESAM-Vitale apparaissent dans : ***C:\INSTALLS\GALSS\32b\Extract\CommonAppData\santesocial\galss\inf***	Figure 82 : Lecteur GIE SESAM-Vitale: Drivers
5	Le .MSI GALSS fournit des drivers 32b et 64b	

Tableau 62 : Lecteur GIE SESAM-Vitale: Procédure d'extraction des drivers

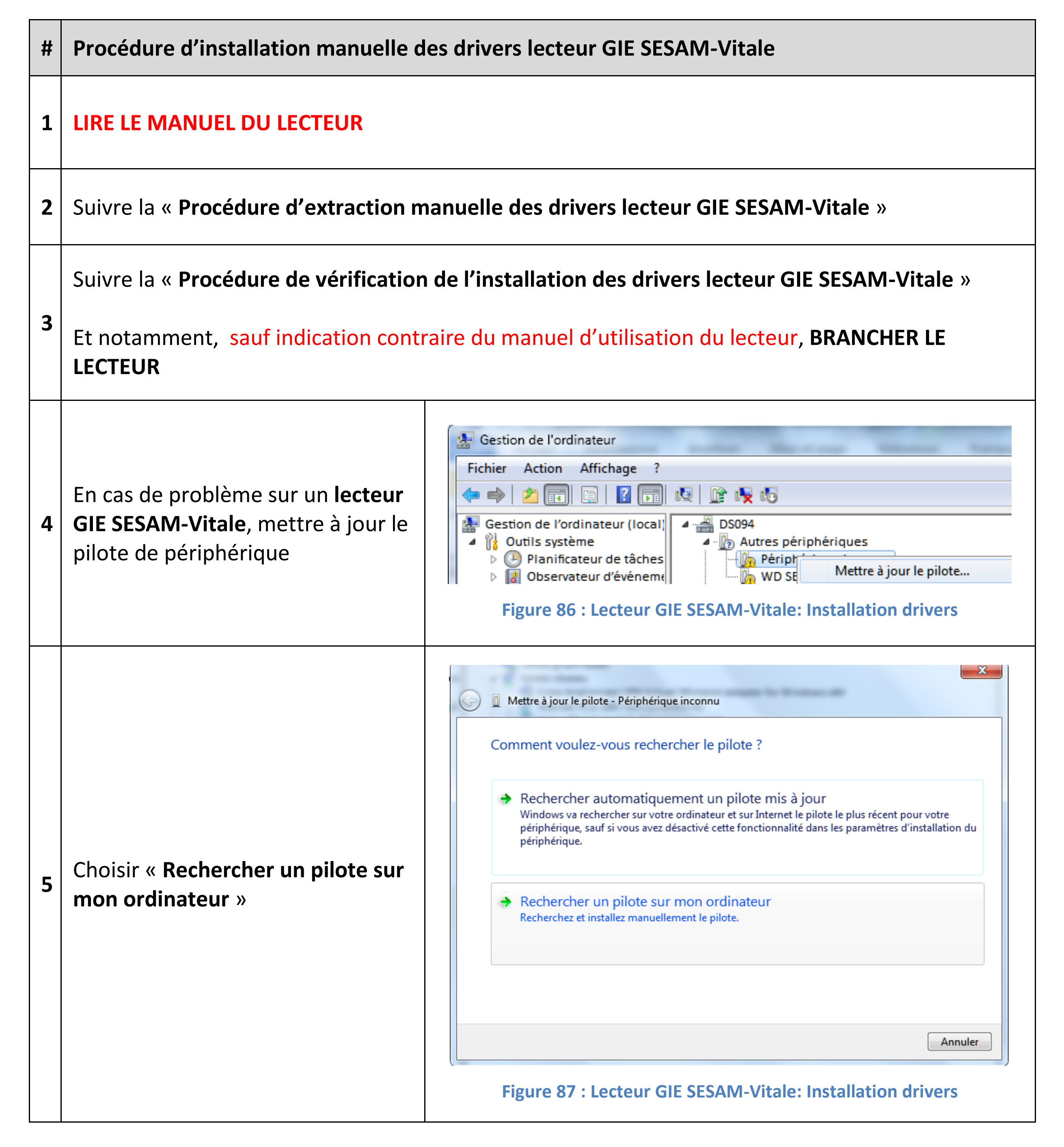
15.2.3.2 *Vérification de l'installation des drivers lecteur GIE SESAM-Vitale*



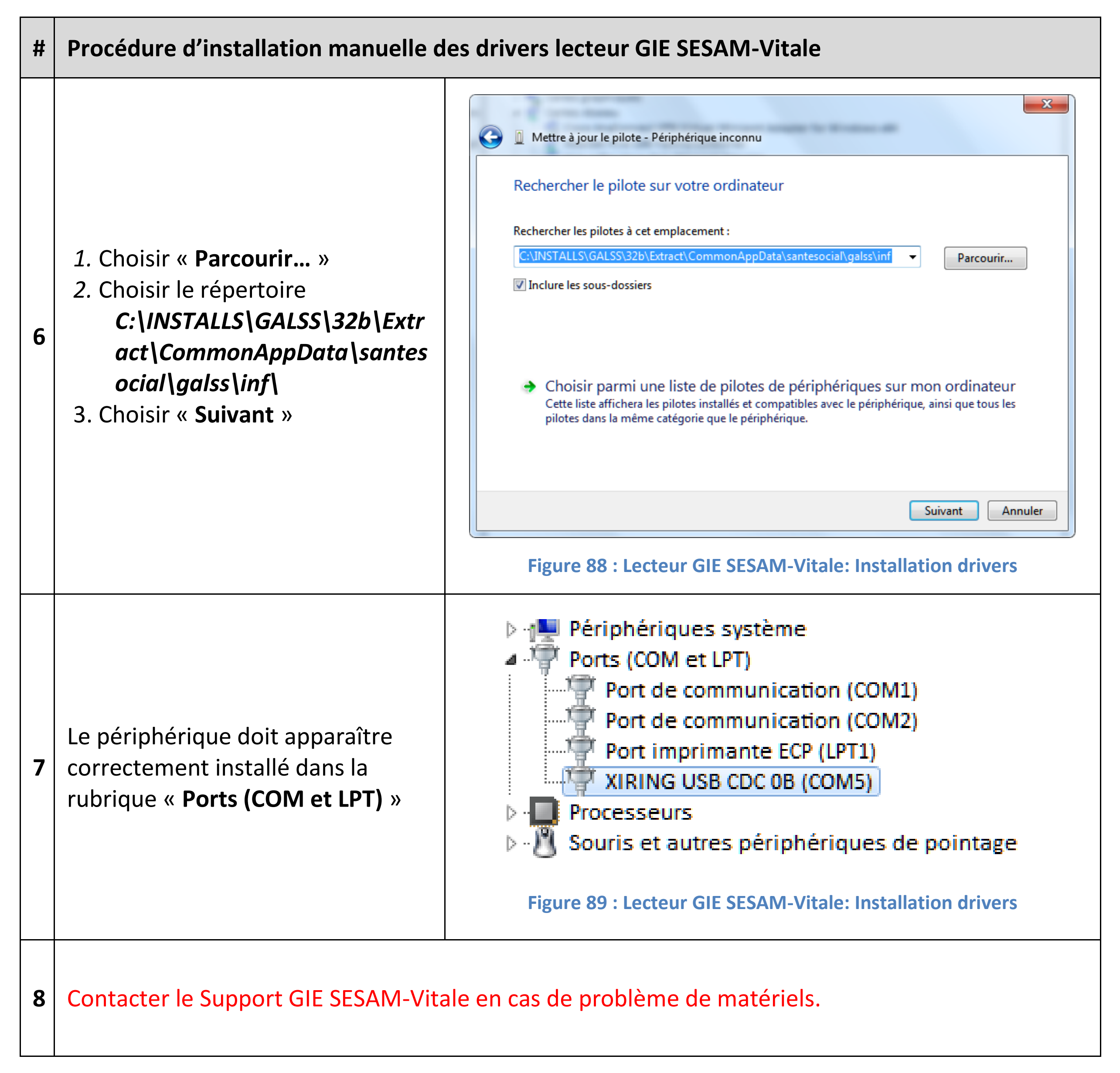
#	Procédure de vérification de l'installation des drivers lecteur GIE SESAM-Vitale	
1	LIRE LE MANUEL DU LECTEUR	
2	Sauf indication contraire du manuel d'utilisation du lecteur, **BRANCHER LE LECTEUR**	
3	Lancer le « **Gestionnaire de périphériques** » : **Touche Windows** > menu de saisie « **Rechercher** » ou « **Exécuter…** » > mmc devmgmt.msc > **Touche** « **entrée** »	Figure 83 : Lecteur GIE SESAM-Vitale: Vérification Installation drivers
4	Problèmes de périphériques	Figure 84 : Lecteur GIE SESAM-Vitale: Vérification Installation drivers
5	Périphériques correctement installés	Figure 85 : Lecteur GIE SESAM-Vitale: Vérification Installation drivers

Tableau 63 : Lecteur GIE SESAM-Vitale: Vérification de l'installation des drivers lecteur GIE SESAM-Vitale

15.2.3.3 Installation manuelle des drivers lecteur GIE SESAM-Vitale



#	Procédure d'installation manuelle des drivers lecteur GIE SESAM-Vitale	
1	LIRE LE MANUEL DU LECTEUR	
2	Suivre la « **Procédure d'extraction manuelle des drivers lecteur GIE SESAM-Vitale** »	
3	Suivre la « **Procédure de vérification de l'installation des drivers lecteur GIE SESAM-Vitale** » Et notamment, sauf indication contraire du manuel d'utilisation du lecteur, **BRANCHER LE LECTEUR**	
4	En cas de problème sur un **lecteur GIE SESAM-Vitale**, mettre à jour le pilote de périphérique	Figure 86 : Lecteur GIE SESAM-Vitale: Installation drivers
5	Choisir « **Rechercher un pilote sur mon ordinateur** »	Figure 87 : Lecteur GIE SESAM-Vitale: Installation drivers



#	Procédure d'installation manuelle des drivers lecteur GIE SESAM-Vitale	
6	*1.* Choisir « **Parcourir…** » *2.* Choisir le répertoire ***C:\INSTALLS\GALSS\32b\Extract\CommonAppData\santesocial\galss\inf*** 3. Choisir « **Suivant** »	Figure 88 : Lecteur GIE SESAM-Vitale: Installation drivers
7	Le périphérique doit apparaître correctement installé dans la rubrique « **Ports (COM et LPT)** »	Figure 89 : Lecteur GIE SESAM-Vitale: Installation drivers
8	Contacter le Support GIE SESAM-Vitale en cas de problème de matériels.	

Tableau 64 : Lecteur GIE SESAM-Vitale: Procédure d'installation manuelle des drivers lecteur GIE SESAM-Vitale

15.2.4 Utilisation avancée du GALSS

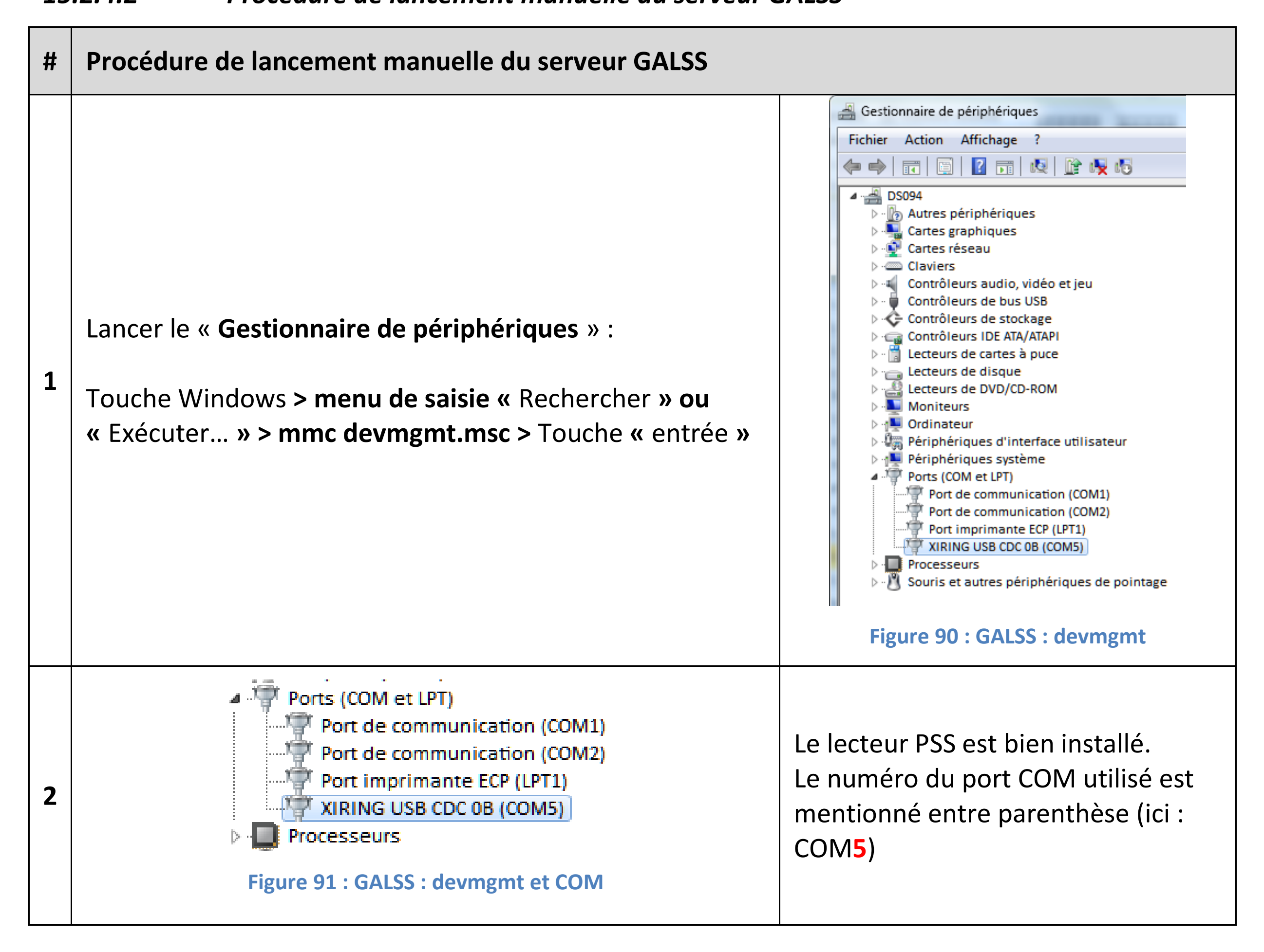
15.2.4.1 Procédure d'arrêt du GALSS

Cette procédure décrit la procédure d'arrêt du GALSS (« tuer le GALSS »).

#	Procédure d'arrêt du GALSS
1	Lancer le « Gestionnaire de tâches » : Touches « **Ctrl + shift + Echap** »
2	Arrêter le processus **CCM.exe** s'il existe
3	Arrêter le processus **galsvw32.exe** ou **galsvw64.exe** s'il existe

Tableau 65 : GALSS : Procédure de lancement manuelle du serveur GALSS

15.2.4.2 Procédure de lancement manuelle du serveur GALSS



#	Procédure de lancement manuelle du serveur GALSS	
1	Lancer le « **Gestionnaire de périphériques** » : Touche Windows **> menu de saisie «** Rechercher **» ou « Exécuter… » > mmc devmgmt.msc >** Touche **«** entrée **»**	Figure 90 : GALSS : devmgmt
2	Figure 91 : GALSS : devmgmt et COM	Le lecteur PSS est bien installé. Le numéro du port COM utilisé est mentionné entre parenthèse (ici : COM5)

<table>
<tr><th>#</th><th colspan="3">Procédure de lancement manuelle du serveur GALSS</th></tr>
<tr><td>3</td><td colspan="2">Ouvrir le fichier galss.ini :

Touche Windows > boîte Rechercher, ou dans la boîte Exécuter > notepad %WINDIR%\galss.ini > Touche « entrée »</td><td>Parcourir le fichier.

Les entrées suivantes doivent apparaître avec un lecteur PSS :

;Protocole PSS
[PROTOCOLE0]
Config=1000,20,15000
NomLib=PSSINW32.DLL

[...]

[CANAL1]
TCanal=1
Index=5
Protocole=0
Caracteristiques=19200,1,8,0,0
NbPAD=1</td></tr>
<tr><td>4</td><td colspan="2">Noter les valeurs TCanal=1, Index=5</td><td></td></tr>
<tr><td>5</td><td colspan="2">Arrêter les processus CCM et galsvwXX.exe :
• « ctrl + shift + echap »
• Sélectionner le tab « Processus »
• Sélection du CCM.exe > Arrêter le processus
• Sélection du galsvwXX.exe > Arrêter le processus</td><td></td></tr>
<tr><td rowspan="3">6</td><td colspan="2">Lancer le processus GALSS serveur en utilisant les valeurs TCanal et Index notées (ici TCanal=1, Index=5)</td><td rowspan="3">Le processus GALSVWXX.exe doit se lancer (attendre quelques secondes)

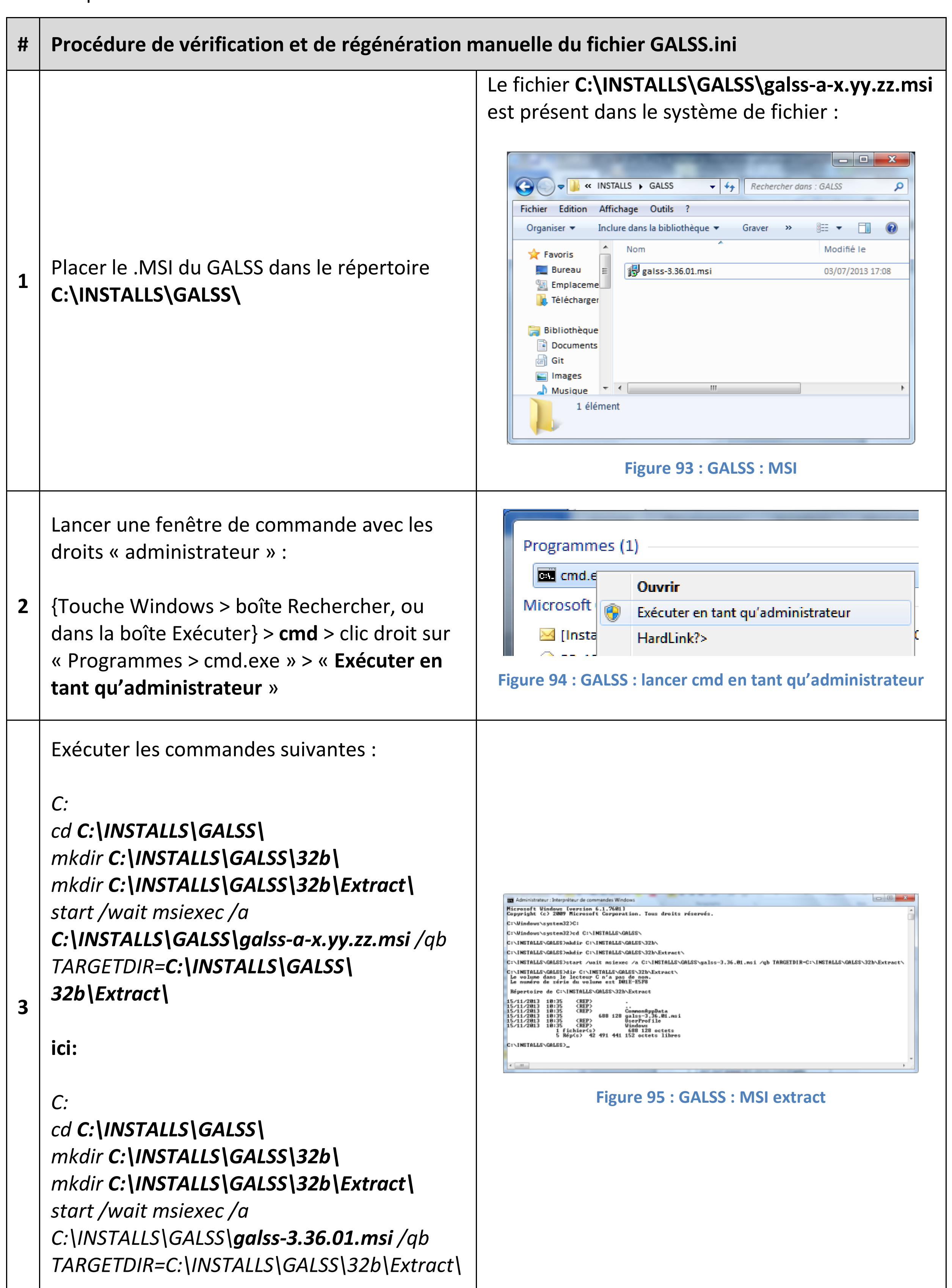
galsvw64.exe
hkcmd.exe

Figure 92 : GALSS : taskmanager</td></tr>
<tr><td>x86</td><td>"%WINDIR%\GALSVW32.EXE" /R /T1 /I5 ("i" majuscule)</td></tr>
<tr><td>x64</td><td>"%ProgramFiles%\santesocial\galss\GALSVW64.EXE"/R /T1 /I5 ("i" majuscule)</td></tr>
<tr><td>7</td><td colspan="2">Relancer le CCM et faire un testssl</td><td>Le testssl doit être OK</td></tr>
</table>

Tableau 66 : GALSS : Procédure de lancement manuelle du serveur GALSS

15.2.4.3 *Procédure de vérification et de régénération manuelle du fichier galss.ini*

Cette procédure est non-intrusive, contrairement à la procédure de régénération du galss.ini décrite dans la partie « installation du GALSS ».



#	Procédure de vérification et de régénération manuelle du fichier GALSS.ini	
1	Placer le .MSI du GALSS dans le répertoire **C:\INSTALLS\GALSS**	Le fichier **C:\INSTALLS\GALSS\galss-a-x.yy.zz.msi** est présent dans le système de fichier : Figure 93 : GALSS : MSI
2	Lancer une fenêtre de commande avec les droits « administrateur » : {Touche Windows > boîte Rechercher, ou dans la boîte Exécuter} > **cmd** > clic droit sur « Programmes > cmd.exe » > « **Exécuter en tant qu'administrateur** »	Figure 94 : GALSS : lancer cmd en tant qu'administrateur
3	Exécuter les commandes suivantes : *C:* *cd **C:\INSTALLS\GALSS*** *mkdir **C:\INSTALLS\GALSS\32b*** *mkdir **C:\INSTALLS\GALSS\32b\Extract*** *start /wait msiexec /a* ***C:\INSTALLS\GALSS\galss-a-x.yy.zz.msi** /qb* *TARGETDIR=**C:\INSTALLS\GALSS*** ***32b\Extract*** **ici:** *C:* *cd **C:\INSTALLS\GALSS*** *mkdir **C:\INSTALLS\GALSS\32b*** *mkdir **C:\INSTALLS\GALSS\32b\Extract*** *start /wait msiexec /a* *C:\INSTALLS\GALSS**galss-3.36.01.msi** /qb* *TARGETDIR=C:\INSTALLS\GALSS\32b\Extract*	Figure 95 : GALSS : MSI extract

#	**Procédure de vérification et de régénération manuelle du fichier GALSS.ini**	
4	Un programme "**ListSerial.exe**" apparait dans **C:\INSTALLS\GALSS\32b\Extract\CommonAppData\santesocial\galssv3** : Exécuter la commande suivante: ***dir C:\INSTALLS\GALSS\32b\Extract\CommonAppData\santesocial\galssv3\ListSerial.exe***	Figure 96 : GALSS : ListSerial
5	Exécuter les commandes suivantes : mkdir %ALLUSERSPROFILE%\santesocial\galssv3\ *copy /Y C:\INSTALLS\GALSS\32b\Extract\Windows\pssinw32.dll C:\INSTALLS\GALSS\32b\Extract\CommonAppData\santesocial\galssv3* *start /wait C:\INSTALLS\GALSS\32b\Extract\CommonAppData\santesocial\galssv3\ListSerial.exe*	Le répertoire %ALLUSERSPROFILE%\santesocial\galssv3\ doit préexister. ListSerial.exe y crée un fichier temporaire PSS_CONFIG.INI et un fichier persistant galss.old ListSerial.exe a besoin de la DLL pssinw32.dll fournie dans la package GALSS pour fonctionner. S'assurer que les ports COM virtuels associés aux lecteurs PSS à détecter ne sont pas ouverts (en particulier le GALSS serveur ne doit pas être lancé).
6	Un fichier "**galss.old**" apparait dans **%ALLUSERSPROFILE%\santesocial\galssv3** Exécuter la commande suivante: ***type %ALLUSERSPROFILE%\santesocial\galssv3\galss.old***	Le contenu du fichier galss.old s'affiche
7	Exécuter la commande suivante: ***echo n|comp.exe %WINDIR%\galss.ini %ALLUSERSPROFILE%\santesocial\galssv3\galss.old***	Le résultat doit être : *Comparaison de C:\Windows\galss.ini et C:\ProgramData\santesocial\galssv3\galss.old...* *Comparaison des fichiers OK*

<table>
<tr><th>#</th><th colspan="2">Procédure de vérification et de régénération manuelle du fichier GALSS.ini</th></tr>
<tr><td></td><td></td><td>Si le résultat est :

Comparaison de C:\Windows\galss.ini et C:\ProgramData\santesocial\galssv3\galss.old...
Les fichiers sont de taille différente.

Les différences doivent être expliquées.</td></tr>
<tr><td rowspan="2">8</td><td rowspan="2">Exécuter la commande suivante:

fc.exe %WINDIR%\galss.ini %ALLUSERSPROFILE%\santesocial\galssv3\galss.old</td><td>Le résultat doit être :
Comparaison des fichiers C:\WINDOWS\galss.ini et C:\PROGRAMDATA\SANTESOCIAL\GALSSV3\GALSS.OLD
FC : aucune différence trouvée</td></tr>
<tr><td>Si des lignes:

***** C:\WINDOWS\galss.ini
Ou
*****
C:\PROGRAMDATA\SANTESOCIAL\GALSSV3\GALSS.OLD

Apparaissent, les différences doivent être expliquées.</td></tr>
<tr><td colspan="3">Contacter le support GIE SESAM-Vitale en cas de problème.</td></tr>
</table>

Tableau 67 : GALSS : Procédure de régénération manuelle du fichier GALSS.ini

Cette procédure, non-intrusive, peut être automatisée :

#	Automatisation de la procédure de vérification et régénération manuelle du fichier GALSS.ini	
1	Lancer une fenêtre de commande avec les droits « administrateur » : Touche Windows > boîte Rechercher, ou dans la boîte Exécuter > **cmd** > clic droit sur « Programmes > cmd.exe » > « **Exécuter en tant qu'administrateur** »	
2	*Set MSI_GALSS_NAME=galss-3.36.01.msi* *Set DIR_WKG=C:\INSTALLS\GALSS* *Rem %DIR_WKG%%MSI_GALSS_NAME% should exist* *cd %DIR_WKG%* *mkdir %DIR_WKG%32b* *mkdir %DIR_WKG%32b\Extract* *start /wait msiexec /a %DIR_WKG%%MSI_GALSS_NAME% /qb TARGETDIR=%DIR_WKG%32b\Extract* *start /wait %DIR_WKG%32b\Extract\CommonAppData\santesocial\galssv3\ListSerial.exe* *echo n|comp.exe %WINDIR%\galss.ini C:\ProgramData\santesocial\galssv3\galss.old* *fc.exe %WINDIR%\galss.ini C:\ProgramData\santesocial\galssv3\galss.old*	Le résultat doit être : *Comparaison des fichiers C:\WINDOWS\galss.ini et C:\PROGRAMDATA\SANTESOCIAL\GALSSV3\GALSS.OLD* *FC : aucune différence trouvée*
3	**En fonction des différences, le fichier galss.ini peut être remplacé sur la base du galss.old:** Copy /Y C:\ProgramData\santesocial\galssv3\galss.old %WINDIR%\galss.ini	
4	**Cette procédure peut faire partie d'une étape de diagnostic du poste**	
5	**Cette procédure permet de détecter les problèmes de configuration du GALSS (lecteur PSS branché sur un port USB où un lecteur PC/SC avait été préalablement branché…)**	
6	**Une fois l'extraction du .MSI effectuée une fois, il n'est plus nécessaire de la refaire. La procédure se réduit à :** *Set DIR_WKG=C:\INSTALLS\GALSS* *start /wait %DIR_WKG%32b\Extract\CommonAppData\santesocial\galssv3\ListSerial.exe* *echo n|comp.exe %WINDIR%\galss.ini C:\ProgramData\santesocial\galssv3\galss.old* *fc.exe %WINDIR%\galss.ini C:\ProgramData\santesocial\galssv3\galss.old*	
Contacter le support GIE SESAM-Vitale en cas de problème.		

Tableau 68 : GALSS : Automatisation de la procédure de vérification et régénération manuelle du fichier GALSS.ini

15.2.4.4 [GALSS 3.40.01+] Activation des traces

Le GALSS 3.40.01 permet d'activer des traces ce qui permet de :

- D'identifier plus facilement l'origine d'un problème GALSS
- De les communiquer au support GIE-SV pour analyse

Se référer au manuel d'installation et d'utilisation du GALSS v1.9.0 **[6]**.

Le GALSS 3.40.02 corrige un problème de performance du 3.40.01 lié à la verbosité des logs.

15.2.5 Cryptolib CPS v5

L'installeur de la Cryptolib CPS v5 permet de fixer des paramètres de fonctionnement en les passant en ligne de commande à l'installeur MSI.

15.2.5.1 Paramètres d'installation proposés par défaut

L'installation par défaut correspond à :

- Installation des composants en mode de détection manuel
- Fréquence de détection des évènements lecteurs en mode automatique à 2sec
- Fréquence de détection des évènements lecteurs en mode manuel à 600 sec

Soit:

[start /wait] msiexec /i CryptolibCPS-xx.yy.zz.msi DETECTIONMODE = 0 WATCHONTIMER = 2 WATCHOFFTIMER = 600 [/qn]

Tableau 69 : Paramétrage par défaut de l'installeur de la Cryptolib CPS v5

15.2.5.2 Paramètres d'installation

Il est possible de « composer » les paramètres disponibles.

Fonction	Commande
Installer les composants en mode détection automatique	[start /wait] msiexec /i CryptolibCPS-xx.yy.zz.msi DETECTIONMODE = 1 [/qn]
Installer les composants en fixant la fréquence de détection des évènements lecteurs en mode automatique	[start /wait] msiexec /i CryptolibCPS-xx.yy.zz.msi WATCHONTIMER = 2 [/qn]
Installer les composants en fixant la fréquence de détection des évènements lecteurs en mode manuel	[start /wait] msiexec /i CryptolibCPS-xx.yy.zz.msi WATCHOFFTIMER = 600 [/qn]
Restaurer en ligne de commande	[start /wait] msiexec /i CryptolibCPS-xx.yy.zz.msi RESTAURE = 1 [/qn]

Fonction	Commande
Installer les composants CPS2ter GALSS	[start /wait] msiexec /i CryptolibCPS-xx.yy.zz.msi CPS2ter = 1 [/qn]
Installer les composants CPS2ter Full PC/SC	[start /wait] msiexec /i CryptolibCPS-xx.yy.zz.msi CPS2ter = 2 [/qn]

Tableau 70 : Paramètres des installeurs de la Cryptolib CPS v5

15.2.5.3 Installation Full PC/SC

v4 Full PC/SC	Cette version est déconseillée, au profit de la **Cryptolib CPS v5**
v5	L'installeur installe automatiquement les composants CPS2ter Full PC/SC : • si le GALSS n'est pas présent (le fichier galsvw32.exe ne doit pas être dans %WINDIR%) • et si la Cryptolib CPS v4 Full PC/SC est présente

Tableau 71 : Installeurs Cryptolib CPS: Critères d'installation de la version Full PC/SC

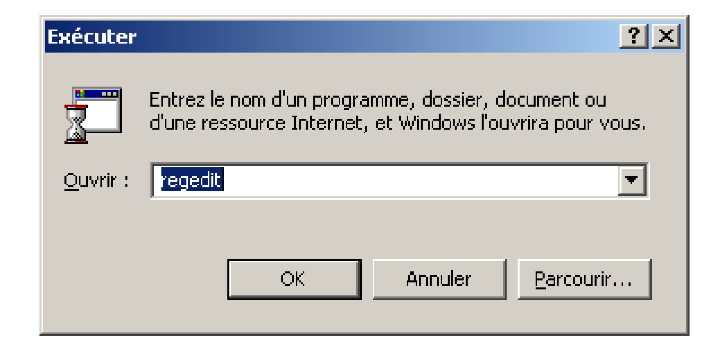
15.2.5.4 Enregistrement manuel du CSP

Le CSP ASIP Santé fourni dans la Cryptolib CPS prend la forme d'une DLL.

L'installeur .MSI de la Cryptolib CPS fourni par ASIP Santé enregistre le CSP ASIP Santé auprès du système conformément aux spécifications de Microsoft.

Le CSP ASIP Santé peut néanmoins être enregistré manuellement et son installation vérifiée en consultant l'entrée suivante de la « base de registre »:

Menu « **Démarrer** » > « **Exécuter… »** > **« regedit** » > « **OK** » (Windows XP) **ou** Menu « **Windows** » > « **Rechercher les programmes ou fichier »** > **« regedit** » > touche « **entrée** » (Windows 7+):



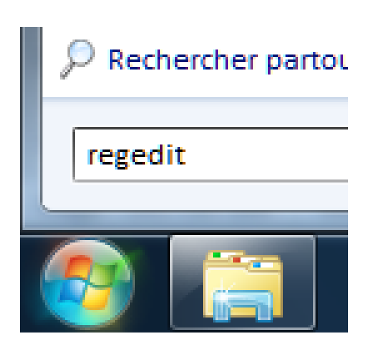


Figure 97 : Windows : Lancement de l'éditeur de base de registre

Archi	Clé
x86 **x64**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider**ASIP Sante Cryptographic Provider**
x64	HKEY_LOCAL_MACHINE\SOFTWARE**Wow6432Node**\Microsoft\Cryptography\Defaults\Provider**ASIP Sante Cryptographic Provider**
x86	historiquement: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider**cps_csp_w32**

Tableau 72 : Clés de registre du CSP ASIP Santé

Valeurs	Type	Défaut	Exemple	Description
Image Path	REG_SZ	%WINDIR%\system32\cps3_csp_w[32|64].dll	C:\Windows\system32\cps3_csp_w64.dll	Chemin vers la DLL du CSP (voir section ci-après)
SigInFile	REG_DWORD	0x00000000	0x00000000	
Type	REG_DWORD	0x00000001	0x00000001	type 1 PROV_RSA_FULL

Tableau 73 : Valeurs pour les clés de registre du CSP ASIP Santé

15.2.5.5 [Windows 7+] Association manuelle de la carte CPx avec le CSP

A partir de Windows Vista, l'OS cherche systématiquement à associer une carte à puce insérée dans un lecteur PC/SC avec un « **pilote de carte à puce** ».

Le pilote de carte à puce est en fait un CSP et l'association se fait sur la base de l'ATR/ATS de la carte.

Cryptolib CPS v5	Seul l'installeur de la Cryptolib CPS v5 assure la déclaration du mapping carte CPx – CSP ASIP Santé

Tableau 74 : Cryptolib CPS v5 : Mapping carte CPx – CSP ASIP Santé

Volet	**Variable**	**Valeur**
Contact	ASIP_SMARTCARDS_CRYPTO	ASIP Sante Cryptographic Provider
	ASIP_SMARTCARDS_TAG	Carte de Professionnel de Sante CPS3
	ASIP_SMARTCARDS_ATR	3b00000000001225006480000000009000
	ASIP_SMARTCARDS_ATRMASK	ff00000000ffffffffffff000000ffffff
Sans contact	ASIP_SMARTCARDS_CRYPTO	ASIP Sante Cryptographic Provider
	ASIP_SMARTCARDS_TAG_CL	Carte de Professionnel de Sante CPS3 - CL
	ASIP_SMARTCARDS_ATR_CL	3B8F80010031B86404B0ECC1739401808290000E
	ASIP_SMARTCARDS_ATRMASK_CL	ffffffffffffffff0000ffc0ffffffffffffffff

Tableau 75 : Variables et valeurs liées aux clés de registre de la carte CPx

L'enrôlement de la carte CPx dans le système se fait sous les clés suivantes :

Archi	**Volet**	**Clé**
x86 x64	Contact	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\%ASIP_SMARTCARDS_TAG%
	Sans contact	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\%ASIP_SMARTCARDS_TAG_CL%
x64	Contact	HKEY_LOCAL_MACHINE\SOFTWARE**Wow6432Node**\Microsoft\Cryptography\Calais\SmartCards\%ASIP_SMARTCARDS_TAG%
	Sans contact	HKEY_LOCAL_MACHINE\SOFTWARE**Wow6432Node**\Microsoft\Cryptography\Calais\SmartCards\%ASIP_SMARTCARDS_TAG_CL%

Tableau 76 : Clés de registre de la carte CPx

Ces clés contiennent les 3 valeurs suivantes:

Valeurs	Type	Défaut	Description
ATRMask	REG_BINARY	%ASIP_SMARTCARDS_ATRMASK[_CL]%	Masque de l'ATR
ATR	REG_BINARY	%ASIP_SMARTCARDS_ATR[_CL]%	ATR
Crypto Provider	REG_SZ	%ASIP_SMARTCARDS_CRYPTO[_CL]%	Chaine de caractère correspondant à la déclaration en base de registre au CSP Asip Santé

Tableau 77 : Clés de registre de la carte CPx

Attention	Ces valeurs sont données à titre documentaire. Elles permettront de vérifier qu'une installation s'est correctement passée ou aux administrateurs de parc de préciser les droits adéquates sur ces clés. **Ces valeurs sont susceptibles de changer sans préavis de la part de l'ASIP Santé.**

Tableau 78 : Point d'attention concernant les valeurs de clés de registre de la carte CPx

Voir aussi en annexe « **Déclaration de la carte Vitale sous Win7** ».

15.2.5.6 Enregistrement du CSP via regsvr32

Au choix exclusif, par ordre de préférence, lancer une console en tant qu'administrateur via le menu « **Démarrer** » > « **Exécuter… »** > « **cmd** » :

#	Version	CSP	Archi	Commande
1	v5	CSP 64-bit	x64	« %windir%\System32\regsvr32.exe %windir%\System32\cps**3**_csp_**w64**.dll »
2	v5	CSP 32-bit	x64	« %windir%**SysWOW64**\regsvr32.exe %windir%**SysWOW64**\cps**3**_csp_**w32**.dll »
3	v5	CSP 32-bit	x86	« %windir%\System32\regsvr32.exe %windir%\System32\cps**3**_csp_**w32**.dll »
4	v4	CSP 32-bit	x86	« %windir%\System32\regsvr32.exe %windir%\System32\cps_csp_**w32**.dll »
5	v4	CSP 32-bit	x64	« %windir%**SysWOW64**\regsvr32.exe %windir%**SysWOW64**\cps_csp_**w32**.dll »
6	v4 Full PC/SC	CSP 32-bit	x86	« %windir%\System32\regsvr32.exe %windir%\System32\cps_csp_**pcsc_w32**.dll »
7	v4 Full PC/SC	CSP 32-bit	x64	« %windir%**SysWOW64**\regsvr32.exe %windir%**SysWOW64**\cps_csp_**pcsc_w32**.dll »

Tableau 79 : Regsvr32 du CSP ASIP Santé

15.3 Installations et utilisations avancées sous Linux

15.3.1 Fedora: Installation d'un lecteur PSS

Fedora	http://forums.fedoraforum.org/showthread.php?t=249170
	http://www.jamesarbrown.com/?p=5

Tableau 80 : Fedora : Source installation périphériques USB/Série

Etape	Description		Détails
1	lsusb		Formatage de la ligne de la sortie de la commande « `lsusb` »: Bus [nBus] Device [nDevice] : ID [vendorID]:[ProductID] [Dénommination produit]
			Ex. : `Bus 00X Device 00Y: ID` **`0000`**`:1111` *`Chaine`*
2	dmesg|tail		Liste des pilotes installés/chargés
3	**Fedora 15-**	`sudo modprobe usbserial vendor=`**`0x0000`** `product=0x1111`	`ll /dev/tty*` renvoie /dev/ttyUSB0 `setserial /dev/ttyUSB0` ne renvoie pas d'erreur

	Fedora 15+
	
	le module usbserial est compilé dans le noyau
		Editer **/etc/default/grub**
		
		A la fin de:
		
		GRUB_CMDLINE_LINUX
		
		Ajouter:
		
		`"usbserial.vendor=`**`0x0000`** `usbserial.product=0×1111"`
			Le fichier ressemble à:
			
			`1.GRUB_DISTRIBUTOR="Fedora"`
			`2.GRUB_DEFAULT=saved`
			`3.`**`GRUB_CMDLINE_LINUX`**`="rd.md=0 rd.dm=0 rd.lvm.lv=vg_office/lv_root quiet SYSFONT=latarcyrheb-sun16 rhgb KEYTABLE=uk rd.luks=0 rd.lvm.lv=vg_office/lv_swap LANG=en_US.UTF-8 usbserial.vendor=`**`0x0000`** `usbserial.product=0x1111"`

	Fedora 16+ grub2 à la place de grub	Mettre à jour la configuration grub	`grub2-mkconfig > /boot/grub2/grub.cfg`
4	Redémarrer la machine		`ll /dev/tty*` renvoie /dev/ttyUSB0

Tableau 81 : Fedora: Installation d'un lecteur PSS

15.3.2 Procédure de vérification du fichier galss.ini

Etape	Description
1	Le fichier **/usr/local/galss/io_comm.ini** contient la déclaration du mapping **/dev/ttyUSB0** <-> **numéro de port COM** via une ligne du type : COM**X**=/dev/ttyUSB0 Le **numéro de port COM** ainsi mappé est à reporter dans le fichier **/usr/local/galss/galss.ini**, suivant la même logique que sous Windows : [CANAL1] TCanal=1 Index=**X** TConnexion=1 Protocole=0 Caracteristiques=19200,1,8,0,0 NbPAD=1

Tableau 82 : Linux: Procédure de vérification du fichier GALSS.ini

16Configuration de la Cryptolib CPS

16.1 Configuration de la Cryptolib CPS sous Microsoft Windows

16.1.1 Paramétrage de la Cryptolib CPS v4

La Cryptolib CPS2Ter se configure via le fichier **%ALLUSERSPROFILE%\santesocial\CPS\coffre\cps_pkcs11_safe.ini**

v4 Full PC/SC	Avec la Cryptolib CPS v4 Full PC/SC, le fichier s'appelle **cps_pkcs11_pcsc.ini**

La section « **config** » regroupe les clés permettant de faire des ajustements sur le fonctionnement des différents modules composant la Cryptolib CPS v4.

La liste des sections et clés permettant de configurer le module Cryptolib CPS v4 est la suivante:

[Section]	Clé	Défaut	Effet
[config][14]	**Configuration des accès lecteurs**		
	tpc_polling_time	1	Délai en secondes entre 2 tests de présence carte effectif
	cps_open_session_max_try	10	Nombre maximum de tentatives d'ouverture de session CPS
	cps_busy_reader_max_try	10	Nombre maximum de tentatives consécutives d'appel à une fonction CPS qui retourne un CR « lecteur occupé »
	cps_busy_reader_try_sleep	1000	Délai en milliseconde entre deux tentatives consécutives d'appel à une fonction CPS qui retourne un CR « lecteur occupé »
[help]	**Configuration du coffre-fort**		
	count	0	0 Pas de coffres-forts en mode secours
[safe]	**Configuration du coffre-fort**		
	directory	.../coffre	Répertoire des coffres-forts
[trace]	**Configuration des traces**		
	directory	.../traces	Répertoire des traces
	level	0	0 : Pas de traces 50 : Trace de niveau DEBUG 100 : Traces de niveau MAX

Tableau 83 : Windows : Paramétrage de la Cryptolib CPS v4

[14] Cette section [config] est facultative et peut être absente du fichier de configuration. Ce sont alors les valeurs par défaut indiquées dans ce tableau qui sont utilisées par le module Cryptolib CPS.



16.1.2 Paramétrage de la Cryptolib CPS v5

Le paramétrage de la Cryptolib CPS v5 permet essentiellement de déterminer le niveau d'expression des logs des échanges avec la carte et PKCS#11.

Les paramètres de configuration supportés avec la Cryptolib CPS v5 sont :

[Section]	Clé	Type	Défaut	Valeurs possibles	Effet
[(HKCU ou HKLM)\Software\ASIP Sante\PKCS11] **Et / Ou** **[HKLM\Software\Wow6432Node\ASIP Sante\PKCS11]**	**Paramétrage des fonctionnalités PKCS#11**				
	Traces	REG_DWORD	0	0 ou 1	Active les traces
	Debug	REG_DWORD[15]	0	0 à 10	Détermine le niveau de traces
	Sign_Hash	REG_DWORD	1	0 ou 1	Active la signature de hash
	tpc_polling_time[16]	REG_DWORD	2	Durée en secondes, supérieure à 2 secondes	Détermine la fréquence d'appel à la commande lecteur "Test présence Carte" du GALSS. L'intervalle minimum est fixé à 2 secondes. Si la valeur dans la base de registre est inférieure, la valeur est ignorée.

[15] REG_DWORD à partir de la Cryptolib CPS v5.0.13 ; REG_SZ pour les versions 5.0.x antérieures

[16] à partir de la Cryptolib CPS v5.0.13

[Section]	Clé	Type	Défaut	Valeurs possibles	Effet
[(HKCU ou HKLM)\Software\ASIP Sante\CSP] **Et / Ou** **[HKLM\Software\Wow6432Node\ASIP Sante\CSP]**	**Paramétrage des fonctionnalités CSP**				
	Traces	REG_DWORD	0	Les valeurs acceptées sont: LOG_LEVEL_NO = 0 LOG_LEVEL_INFO >= 10 LOG_LEVEL_DEBUG >= 40 LOG_LEVEL_MAX >= 50	Active les traces et fixe le niveau de traces
[(HKCU ou HKLM)\Software\ASIP Sante\CCM] **Et / Ou** **[HKLM\Software\Wow6432Node\ASIP Sante\CCM]**	**Paramétrage des fonctionnalités CCM**				
	autoDetect	REG_DWORD	0	0 ou 1	Active le mode détection automatique
	watchOffTimer	REG_ DWORD	0x00000258 (600)	Durée en secondes	Fixe la fréquence (en seconde) de détection des évènements lecteurs en mode manuel
	watchOnTimer	REG_DWORD	0x00000002 (2)	Durée en secondes	Fixe la fréquence (en seconde) de détection des évènements lecteurs en mode automatique

Tableau 84 : Windows : Paramétrage de la Cryptolib CPS v5

Choix de la [Section] à renseigner en Base de registre :

- **HKCU ou HKLM** : le paramétrage est effectif pour l'utilisateur courant (HKCU) ou pour l'ensemble des utilisateurs du poste (HKLM). Si les 2 clés sont positionnées, le paramétrage de HKCU prime sur celui de HKLM.
- **Wow6432Node** : concerne uniquement la clé HKLM sur les OS 64 bits. Sa présence indique un paramétrage effectif pour les applications 32 bits uniquement. Son absence indique un paramétrage effectif pour les applications 64 bits uniquement. Les 2 paramétrages peuvent être cumulés.

16.1.3 Paramétrage d'Internet Explorer : mode protégé amélioré (EPM)

16.1.3.1 Accès aux paramètres via l'interface Microsoft Windows

4 paramètres sont déterminants sur le mode de fonctionnement d'Internet Explorer et par contrecoup sur l'utilisation de la carte CPx via ce navigateur. Ces paramètres sont :

1. UAC : User Account Control
2. PM : Protected Mode
3. EPM : Enhanced Protected Mode
4. EPM-64b : Enhanced Protected Mode 64b

Ils correspondent à des paramètres mis en place par Microsoft pour améliorer la sécurité de ses systèmes.

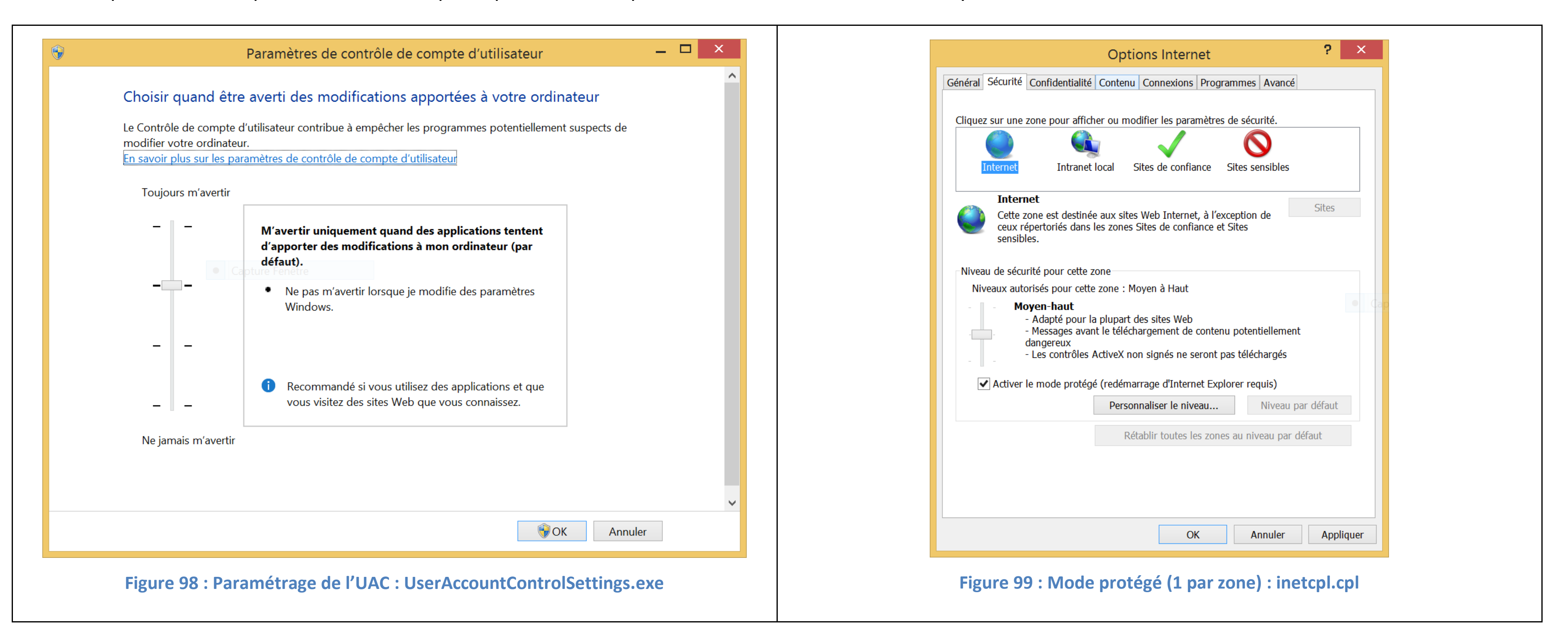


Figure 98 : Paramétrage de l'UAC : UserAccountControlSettings.exe

Figure 99 : Mode protégé (1 par zone) : inetcpl.cpl

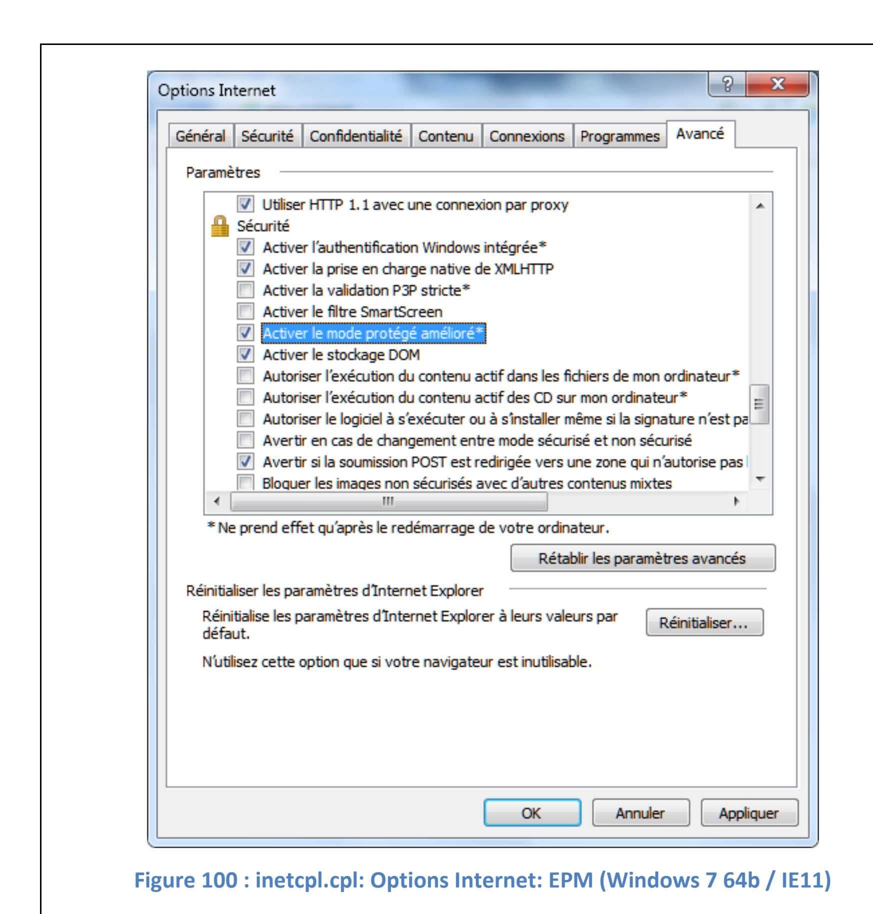


Figure 100 : inetcpl.cpl: Options Internet: EPM (Windows 7 64b / IE11)

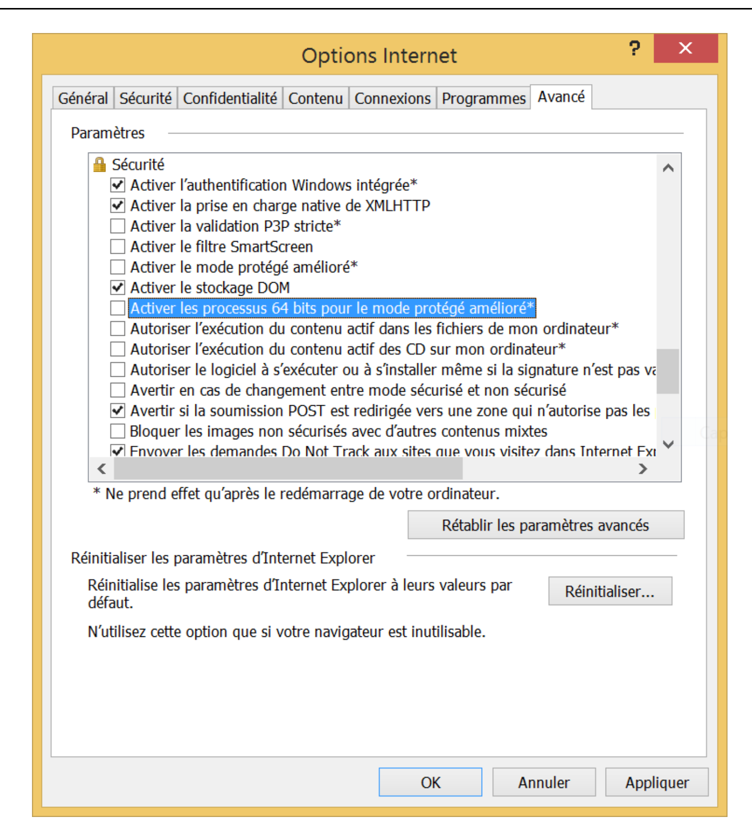


Figure 101 : inetcpl.cpl : Options Internet : EPM et EPM (64b) (Windows 8 et Windows 8.1 / IE11)

16.1.3.2 Activation de l'EPM : incidence sur la fenêtre de saisie du code porteur

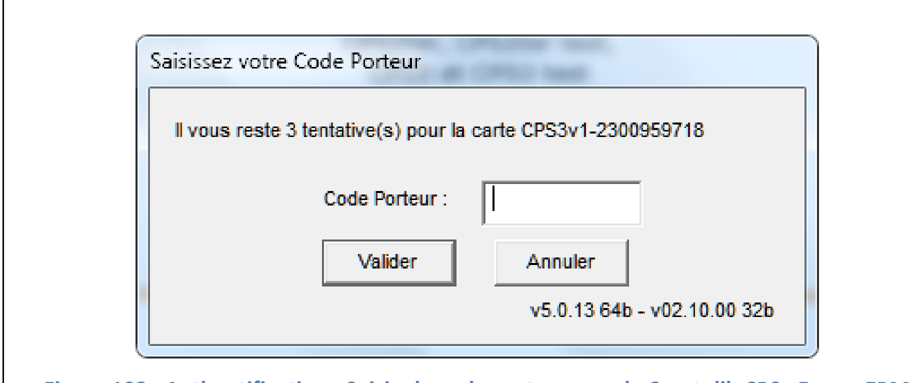


Figure 102 : Authentification : Saisie du code porteur avec la Cryptolib CPS v5 sans EPM

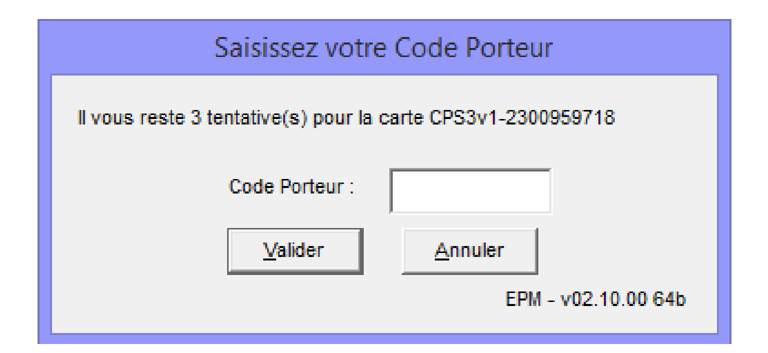


Figure 103 : Authentification : Saisie du code porteur avec la Cryptolib CPS v5 avec EPM

16.1.3.3 Incidence du paramétrage du mode protégé amélioré (EPM) sur les accès vers la carte CPx

Les mentions « activé » / « désactivé » documentent le paramétrage par défaut. Le tableau commente les effets d'un changement du paramétrage par défaut.
La couleur **verte** indique qu'aucun problème n'a été relevé. La couleur **rouge** indique un point d'attention. Les **cases grisées** analysent l'impact d'un changement de paramétrage par défaut.

		Windows 7		**Windows 8**		**Windows 8.1**	
		x86	**x64**	**x86**	**x64**	**x86**	**x64**
UAC		activé	activé	activé	activé	activé	activé
IE9	**PM (*)**	activé	activé	N/A			
	EPM	N/A					
	EPM-64b						
IE10	**PM (*)**	activé	activé	activé	activé	activé	activé
	EPM	N/A	désactivé L'activation de l'EPM passe IE en **64b <u>si</u> l'UAC est activé** en parallèle. **Si EPM activé et UAC activé :** Clib CPS v5 64b requise, GALSS 64b requis Carte CPS dans lecteur PC/SC : OK Carte CPS dans lecteur PSS : OK (GALSS x64)	désactivé L'activation de l'EPM ne détermine pas l'architecture de IE: **avec l'EPM activé, iexplore.exe fonctionne en 32b.** **Si EPM activé :** Cryptolib CPS v5 x32 OK, GALSS x32 KO Carte CPS dans lecteur PC/SC: OK Carte CPS dans lecteur PSS: KO	désactivé	N/A	
	EPM-64b	N/A	N/A	N/A	désactivé **Si EPM-64b activé :** Cryptolib CPS v5 64b requise, GALSS 64b requis mais GALSS 64b KO Carte CPS dans lecteur PC/SC : OK Carte CPS dans lecteur PSS : KO		
IE11	**PM (*)**	activé	activé	activé	activé	activé	activé
	EPM	désactivé N/A	désactivé L'activation de l'EPM passe le ContentManager **iexplore.exe** en **64b <u>si</u> l'UAC est activé** en parallèle. **Si EPM activé et UAC activé :** Clib CPS v5 64b requise, GALSS 64b requis Carte CPS dans lecteur PC/SC : OK Carte CPS dans lecteur PSS : OK (GALSS x64)	désactivé L'activation de l'EPM ne détermine pas l'architecture du ContentManager iexplore.exe : **avec l'EPM activé, iexplore.exe fonctionne en 32b.** **Si EPM activé :** Cryptolib CPS v5 x32 fonctionne, GALSS x32 ne fonctionne pas Carte CPS dans lecteur PC/SC: OK Carte CPS dans lecteur PSS : KO	désactivé	activé (**)	activé (**)
	EPM-64b	N/A	N/A	N/A	désactivé **Si EPM-64b activé :** Cryptolib CPS v5 64b requise, GALSS 64b requis mais GALSS 64b KO Carte CPS dans lecteur PC/SC : OK activé : Carte CPS dans lecteur PSS : KO	N/A	désactivé **Si EPM-64b activé :** Cryptolib CPS v5 64b requise, GALSS 64b requis mais GALSS 64b KO Carte CPS dans lecteur PC/SC : OK Carte CPS dans lecteur PSS : KO

Tableau 85 : Windows : Installation par défaut Internet Explorer, UAC, PM et EPM

(*) Le mode protégé (**PM**) est activé par défaut sur la zone « **Internet** » (**) Remis en cause par: https://technet.microsoft.com/en-us/security/bulletin/ms13-088 (KB2888505)



16.1.4 GPO et ADM

L'utilisation de GPO ou d'ADM(X) est préconisée sous Windows en lieu et place des accès directs en base de registre afin de paramétrer les comportements de l'OS.

#	Description
1	Configuration des mises à jour automatiques
2	Configuration de la recherche automatique des drivers
3	Configuration de l'affichage des erreurs critiques aux utilisateurs
4	Configuration des zones de sécurités Internet Explorer
5	Configuration des comportements carte et cryptographique
6	Configuration des comportements carte et cryptographique MS Office

Tableau 86 : Principales GPOs



16.2 Configuration de la Cryptolib CPS sous Linux

16.2.1 Paramétrage de la Cryptolib CPS v4

La Cryptolib CPS2Ter se configure via le fichier **/etc/opt/santesocial/CPS/cps_pkcs11_safe.ini**

La grammaire du fichier est la même que sous Windows (cf. plus haut).

16.2.2 Paramétrage de la Cryptolib CPS v5

Le paramétrage de la Cryptolib CPS v5 permet essentiellement de déterminer le niveau d'expression des logs des échanges avec la carte et PKCS#11.

Les paramètres de configuration supportés avec la Cryptolib CPS v5 sous Linux sont :

[Section]	Clé	Type	Défaut	Valeurs possibles	Effet
	Paramétrage des fonctionnalités PKCS#11				
Variable d'environnement	CPS3_PKCS11_TRACES	boolean	N/A	true ou false	Active les traces
	CPS3_DEBUG	string	N/A	N/A ou 10	Détermine le niveau de traces

/etc/opt/santesocial/CPS/cps3_pkcs11.conf	Sign_Hash
	{
	active = true;
	}
		boolean	active = true;	true ou false	Active la signature de hash

Tableau 87 : Linux : Paramétrage de la Cryptolib CPS v5



16.3 Configuration de la Cryptolib CPS sous Apple Mac OS X

16.3.1 Paramétrage de la Cryptolib CPS v5

Avec l'installeur PKG v5.0.7 pour Mac OS X, le fichier de configuration **cps3_pkcs11.conf** se trouve dans le dossier **/Library/Preferences/santesocial/CPS/**

Les paramètres de configuration supportés avec la Cryptolib CPS v5 sous Mac OS sont :

<table>
<tr><th>[Section]</th><th colspan="2">Clé</th><th>Type</th><th>Défaut</th><th>Valeurs possibles</th><th>Effet</th></tr>
<tr><td rowspan="2">/Library/Preferences/santesocial/CPS/cps3_pkcs11.conf</td><td rowspan="2">traces
{
active = false;
debug = 0;
}</td><td>active</td><td>boolean</td><td>active = false;</td><td>true ou false</td><td>active les traces de l’interface PKCS11 cps3p11_*.log</td></tr>
<tr><td>debug</td><td>string</td><td>debug = 0;</td><td>N/A, 0 ou 10</td><td>active les traces internes cps3opsc_*.log</td></tr>
</table>

Tableau 88 : Mac OS : Paramétrage de la Cryptolib CPS v5



16.3.2 Edition des fichiers de configuration

Ce chapitre s'applique en particulier à l'édition du fichier de configuration **cps3_pkcs11.conf**.

Si les droits du fichier sont correctement définis, l'édition de ce fichier avec TextEdit ne pose pas de problème. La méthode pour sauvegarder un fichier texte avec TextEdit avec un nom d'extension personnalisé est la suivante :

Dans TextEdit, quand on a édité un nouveau fichier et qu'on veut le sauvegarder au format texte, il faut :

1. Dans les préférences "TextEdit -> Préferences -> Onglet Ouverture et enregistrement"
    a. décocher l'option "ajouter une extension .txt aux fichiers au format Texte"
2. Dans le menu "TextEdit -> Format" sélectionner "Convertir au format Texte"
3. Lors de la sauvegarde du fichier:
    a. l'encodage par défaut doit être "Unicode (UTF8)"
    b. indiquer l'extension souhaitée
    c. sauvegarder.

Il est possible de supprimer l'extension .txt a posteriori en éditant les propriétés du fichier avec (cmd+i ou pomme+i) dans le Finder.



16.4 Fichiers de traces

Chaque fichier de trace est activable de manière indépendante.

16.4.1 Formats des fichiers de traces

Système	Fichiers		Exemple	Signification	Détails
Windows	**V4**	cps_ccm_[pid]_[tid].log	cps_ccm_b4c_718.log	Traces CCM	[pid]: Process ID [tid]: Thread ID
		cps_csp_[pid]_[tid].log	cps_csp_b4c_718.log	Traces CSP	
		cpspkcs11_[pid]_[tid].log	cpspkcs11_b4c_718.log	Trace PKCS#11	
	V5	cps3_csp_[pid]_[tid].log	cps3_csp_d84_db4.log	Traces CSP	
		cps3opsc_[pid]_[tid].log	cps3opsc_d84_db4.log	Trace OpenSC	
		cps3p11_[pid]_[tid].log	cps3p11_d84_db4.log	Trace PKCS#11	
Mac OS X	**V5**	cps3opsc_[pid]_[tid].log	cps3opsc_d84_db4.log	Trace OpenSC	
		cps3p11_[pid]_[tid].log	cps3p11_d84_db4.log	Trace PKCS#11	
Linux					

Tableau 89 : Cryptolib CPS : Format des fichiers de traces

Les processus appelants apparaissent en entête de certains fichiers du lot de traces (le premier fichier du triplet {process ; pid ; tid}. Par exemple :

```
Fri Nov 15 17:01:23.725 : Process = "C:\Program Files\santesocial\CPS\CCM.exe"
Fri Nov 15 16:59:01.606 : getTraceConf:Command line : "LogonUI.exe" /flags:0x0
```

Tableau 90 : Cryptolib CPS : Mention du procesus parent dans les fichiers de traces

16.4.2 Emplacements des fichiers de traces

Lorsque l'on quitte CPS-Gestion en sauvegardant les fichiers journaux :

- CPS-JOUR.TXT
- CPS-INFO.TXT
- CPS-DIAG.TXT
- CPS-TRAC.TXT

ou lorsque les traces de la Cryptolib CPS ont été activées :

- Cryptolib CPS v4
  - clé *level* dans la section [trace] du fichier de configuration **cps_pkcs11_safe.ini** décrit ci-dessus
- Cryptolib CPS v5
  - clé *Traces* et *Debug* de l'entrée **[(HKCU ou HKLM)\Software\ASIP Sante\]** de la base de registre décrit ci-dessus

L'emplacement des fichiers de traces par défaut est le suivant :

Système	Version de la Cryptolib CPS	Version du Système	Répertoire
Windows	A partir du setup Cryptolib CPS v3.06	sous Windows XP ou 2000[17]	C:\Documents and settings\All Users\Application Data\santesocial\cps\log\
		A partir de Windows Vista	1. %ALLUSERSPROFILE%\santesocial\CPS\log\ 2. %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\Virtualized\C\ProgramData\santesocial\cps\log\ 3. %PUBLIC%\AppData\santesocial\cps\log\
Mac OS X			/Library/Logs/santesocial/CPS/
Linux	Fichiers traces de la Cryptolib CPS		/var/opt/santesocial/CPS/log/
	Fichiers journaux de CPS-Gestion (A partir du setup Cryptolib CPS v3.06)		

Tableau 91 : Cryptolib CPS : Emplacement des fichiers de traces

[17] `Application Data` est un dossier caché par défaut sous Windows XP et Windows 2000



16.4.3 Crashdumps

Les exécutables Windows génère des fichiers « Crashdump » à l'emplacement suivant :

%USERPROFILE%\AppData\Local\Microsoft\Windows\WER\ReportArchive\

Tableau 92 : Windows: Emplacement des fichiers de crashdump

Ainsi, le CCM.exe, par exemple, génère des fichiers de traces en cas de Crash dans le répertoire :

%USERPROFILE%\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_CCM.exe_XXXXXXXXXXXXXXXXXX\

Tableau 93 : CCM: Emplacement des fichiers de crashdump

Ces fichiers peuvent être demandés pour analyse.

17 Mises à jour et désinstallations de la Cryptolib CPS

17.1 Mises à jour et désinstallations de la Cryptolib CPS sous Windows

17.1.1 GALSS

17.1.1.1 Mise à jour du fichier galss.ini

Le fichier **galss.ini** n'est pas remis à jours au « fil de l'eau » : son contenu est figé lorsque l'installation du GALSS s'achève. Afin de le mettre à jour, il faut appliquer la procédure suivante :

#	GALSS : Procédure de mise à jour du fichier galss.ini
1	**Connecter le/les lecteur(s) de cartes au poste de poste de travail**
2	**Appliquer la procédure « GALSS : Procédure de sauvegarde du fichier galss.ini » <u>en supprimant manuellement</u> les fichiers galss.ini**
3	<u>Relancer</u> l'installation du GALSS: 1. Double-cliquer sur le .MSI d'installation 2. L'installeur passe en mode "réparation" 3. L'installeur relance l'utilitaire de détection des lecteurs de carte 4. Le fichier galss.ini est recréé en conséquence
4	Si le poste est correctement configuré pour Java: 1. Remplacer l'étape 3 par un diagnostic et une installation ODI

Tableau 94 : GALSS : Procédure de mise à jour du fichier galss.ini

17.1.1.2 Désinstallation

Cf. **[6] « GALSS v3.xx Gestionnaire d'accès aux lecteurs Santé Social »**

La désinstallation du GALSS ne détruit pas le fichier galss.ini.
Il est donc inutile de désinstaller le GALSS dans l'espoir de régénérer sa configuration lecteur. Pour mettre à jour la configuration lecteur, il faut appliquer la procédure « **GALSS: régénération du fichier galss.ini »**.

Tableau 95 : GALSS : Remarque désinstallation sous Windows

La procédure de désinstallation complète du GALSS sous Windows est la suivante :

#	GALSS : Procédure de désinstallation complète du GALSS
1	Arrêter tous les processus liés au GALSS : • Navigateurs • LPS • CCM • galsvw32.exe • galsvw64.exe
2.1	Désinstaller le GALSS via 1. Panneau de configuration 2. Programmes et fonctionnalités 3. Désinstaller ou modifier un programme 4. Sélectionner « GALSS v3.3x » 5. Cliquer sur « Désinstaller »
2.2	Désinstaller le GALSS via la ligne de commande: `[start /wait] msiexec /x msi_name [/qn]`
2.3	Ou via la ligne de commande: `[start /wait] msiexec /x {674C6EFF-8591-48AB-94AB-D9DC35F9BB5E} [/qn]`
3	Appliquer la procédure « **GALSS : Procédure de sauvegarde du fichier galss.ini** » en supprimant les fichiers galss.ini (le désinstalleur du GALSS ne supprime pas les fichiers galss.ini).

Tableau 96 : GALSS : Procédure de désinstallation complète sous Windows

17.1.2 Cryptolib CPS

17.1.2.1 Montée de version

La procédure de montée de version de la Cryptolib CPS sous Windows est la suivante:

#	Cryptolib CPS : Procédure de mise à jour de la Cryptolib CPS
1	Exécuter le package d'installation de la Cryptolib CPS cible. L'installeur se charge de détecter les versions de la Cryptolib CPS déjà présentes, de mettre à jour la Cryptolib CPS vers la version cible et de mettre à jour les informations dans le système.

Tableau 97 : Cryptolib CPS : Procédure de mise à jour sous Windows

17.1.2.2 Désinstallation

Les procédures de désinstallation de la Cryptolib CPS sous Windows sont les suivantes, au choix:

#	Cryptolib CPS : Procédure de désinstallation complète de la Cryptolib CPS
1	Exécuter le package d'installation de Cryptolib CPS de la même manière que lors de la phase d'installation. La confirmation de la désinstallation est demandée.
2.1	Désinstaller la Cryptolib CPS via 1. Panneau de configuration 2. Programmes et fonctionnalités 3. Désinstaller ou modifier un programme 4. Sélectionner « **Composants cryptographiques CPS vx.y.z (architecture)** » 5. Cliquer sur « Désinstaller »
2.2	Désinstaller la Cryptolib CPS via la ligne de commande: `[start /wait] msiexec /x msi_name [/qn]`
2.3	Ou via la ligne de commande: `[start /wait] msiexec /x {4748C15E-92F4-4FE8-BB47-6234D0CAE49B} [/qn]`
2.4	Supprimer les logs (cf. « Emplacements des fichiers de traces »)
2.5	Vider le cache (cf. « Sécurité / Cache de fichier carte »)

Tableau 98 : Cryptolib CPS : Procédure de désinstallation complète sous Windows

17.1.3 Windows Update

<table>
<tr><th>#</th><th colspan="3">Commentaires Windows Update</th></tr>
<tr><td>1</td><td colspan="3">L'ASIP Santé ne distribue pas de composants logiciels via Windows Update.</td></tr>
<tr><td>2</td><td colspan="3">Certains périphériques peuvent avoir besoin de Windows Update pour s'installer correctement (lecteur de carte à puces ou cartes à puce).</td></tr>
<tr><td>3</td><td colspan="3">Sous Windows 7, la Cryptolib CPS enregistre un CSP et l'associe en base de registre aux cartes CPx de sorte que le message « pilote de carte à puce non trouvé » ne s'affiche plus au moment de l'insertion d'une carte CPx dans un lecteur PC/SC.</td></tr>
<tr><td>4</td><td colspan="3">Sous Windows 7+, les messages « pilote de carte à puce non trouvé » s'affichent lors d'une insertion de carte CPx:
Sous Windows 7 x86, si la Cryptolib CPS v4 (32b) est installée
La Cryptolib CPS v4 n'associe pas les ATR des cartes CPx au CSP
Sous Windows 7 x64, si la Cryptolib CPS v4 (32b) ou si la Cryptolib CPS v5 32b sont installés
Dans ces cas, aucun CSP « natif / 64b » n'est installé
Pour éviter ces messages, il est nécessaire d'installer la Cryptolib CPS v5 dans sa version destinée à l'architecture de l'OS courant

Voir aussi section « [Windows 7+] Association manuelle de la carte CPx avec le CSP ».</td></tr>
<tr><td>5</td><td colspan="3">La configuration de Windows Update sur le poste doit être précisément maitrisée afin d'éviter toute déconvenue liée à une montée de version induite par une mise à jour du système.</td></tr>
<tr><td>6</td><td colspan="3">Pour les usages professionnels, la recommandation est de se rapprocher d'un environnement dit « qualifié ».</td></tr>
<tr><td>7</td><td colspan="3">Un « environnement qualifié » est un environnement dont :
la configuration est tout le temps connue en tout point (ex. : Win7 SP1 build…, IE10 build…)
la configuration a été validée pour un périmètre fonctionnel connu en tout point (DMP version 1.0.1 fonctionnant avec Win7 SP1 build…, IE10 build…)
la configuration de mise à jour est validable sans impact sur les environnements de production
les processus de mise à jour et de retour arrière sont connus et eux-mêmes validés</td></tr>
<tr><td>8</td><td>Exemple de stratégie pour un poste isolé</td><td>Windows Update : désactivé</td><td>Pas de mise à jour intempestive.

Mises à jour manuelles régulières sur des créneaux temporels dédiés afin de bien valider les conditions de départ, de bien suivre les redémarrages…</td></tr>
</table>

#	Commentaires Windows Update		
9	Exemple de stratégie pour un parc de postes	Windows Update : programmé	Pas de mise à jour intempestive sur les postes. Configuration de serveurs de mises à jour sur le réseau local (WSUS). Machines de tests et d'homologation des mises à jour.

Tableau 99 : Commentaires Windows Update

#	Exemple de paramétrage de Windows Update sous Windows 7

1	`rem Device Software Installation, 0 au lieu de 1`
	
	`reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DriverSearching" /v "SearchOrderConfig" /t REG_DWORD /d 0 /f`

2	`rem Windows Update, 1 au lieu de 4`
	
	`reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v "AUOptions" /t REG_DWORD /d 1 /f`

Tableau 100 : Paramétrage de Windows Update sous Windows 7

Les documents de référence sur ces aspects sont

#	Aspect	Documentation de référence
1	Installation de matériels	Step-By-Step Guide to Controlling Device Installation Using Group Policy
2	Windows Update	Windows Server Update Services (conseillé en SI ES) Configure Automatic Updates by Using Group Policy

Tableau 101 : Documentation de référence

17.2 Mises à jour et désinstallations de la Cryptolib CPS sous Linux

17.2.1 Cryptolib CPS

17.2.1.1 Montée de version

La procédure de montée de version de la Cryptolib CPS sous Linux est la suivante:

#	Cryptolib CPS : Procédure de mise à jour de la Cryptolib CPS	
1	rpm	`rpm -U[vh] CryptolibCPS-x.y.z-i386.rpm`
	Dpkg	Appliquer la procédure d'installation (`dpkg -i`)

Tableau 102 : Cryptolib CPS : Procédure de mise à jour sous Linux

17.2.1.2 Désinstallation de la Cryptolib CPS

La procédure de désinstallation de la Cryptolib CPS sous linux est la suivante:

#	Cryptolib CPS : Procédure de désinstallation complète de la Cryptolib CPS	
1	rpm	`rpm -qa	grep -i cryptolib` `rpm -qa	grep -i Cryptolib` `rpm -e <package name>`
	dpkg	`[sudo] dpkg -D 3777 --force-all --purge cryptolibcps > /tmp/logs-cryptolibcps-uninstall.txt 2>&1`

Tableau 103 : Cryptolib CPS : Procédure de désinstallation complète sous Linux

18 Performances et sécurité

18.1 Vérification des fournitures ASIP Santé

<table>
<tr><th>#</th><th colspan="3">Remarque</th><th colspan="2">Précisions</th></tr>
<tr><td>1</td><td colspan="5">Les fournitures ASIP Santé sont signées.
L'authenticité et l'intégrité des fournitures ASIP Santé peuvent ainsi être vérifiées.</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Windows</td><td colspan="2" rowspan="2"><code>signtool.exe verify /pa [PATH_TO]\file_to_be_verified</code></td><td>OK</td><td>Successfully verified:
[PATH_TO]\file_to_be_verified</td></tr>
<tr><td>KO</td><td>SignTool Error: No signature found.
SignTool Error: File not valid:
[PATH_TO]\file_to_be_verified

Number of errors: 1</td></tr>
<tr><td rowspan="5">4</td><td rowspan="5">Linux</td><td rowspan="4">rpm</td><td rowspan="2"><code>rpm -Kvv --nosignature <rpm-file></code></td><td>OK</td><td><rpm-file>: md5 OK</td></tr>
<tr><td>KO</td><td></td></tr>
<tr><td rowspan="2"><code>rpm --checksig <rpm-file></code></td><td>OK</td><td><rpm-file>: size pgp md5 OK</td></tr>
<tr><td>KO</td><td></td></tr>
<tr><td>dpkg</td><td>Vérifier le .RPM avant le de convertir.</td><td>N/A</td><td>N/A</td></tr>
</table>

Tableau 104 : Vérification des fournitures ASIP Santé

18.2 Certificats et clés privées

#	Certificats et clés privées	
1	**Certificats**	Un certificat associe 3 éléments essentiels : 1. Une clé publique (au sens cryptographique du terme) 2. Des informations d'identité (identité du porteur de carte CPx dans le cas de l'IGC de Santé) 3. Des informations permettant de vérifier son statut (date d'émission, date d'expiration, numéro de série…) Comme son nom l'indique, **la clé publique peut être diffusée en clair** (de fait, le rôle de cette clé consiste justement à être diffusée en clair). Quant aux informations d'identité associées à la clé publique au sein du certificat, **elles sont elles aussi destinées à être transmises en clair**. Fonctionnellement, elles sont disponibles en accès libre (via les Ordres ou les annuaires de santé). Les informations contenues dans un certificat ne donc sont pas sensibles. **Les certificats peuvent être diffusés en clair sans crainte.**
2	**Clé privée**	Une clé privée est associée à une clé publique, elle-même généralement associée à une identité au sein d'un certificat. Cette association {clé privée ; certificat = {clé publique ; identité}} est assurée en premier lieu par et dans la carte CPx. **Une clé privée est une donnée sensible**. La carte CPS3 héberge 3 clés privées (authentification, signature et technique) **qui ne « sortent » jamais de la carte.** Les middlewares cryptographiques assurent eux aussi une association {clé privée ; certificat}, généralement **par l'intermédiaire de la mise en œuvre d'un identifiant de clé privée**. La Cryptolib CPS demande ainsi la réalisation d'opérations cryptographiques à la carte CPx en lui précisant des identifiants de clé privée, et non en exportant les clés privées pour les manipuler en dehors de la carte. La carte CPx autorise ou, au contraire, interdit certaines opérations cryptographiques avec les clés privées : l'opération de signature est ainsi seulement autorisée avec l'identifiant de clé privée de signature. Au contraire, les opérations de déchiffrement de données ou d'export de clé privée sont tout simplement interdites. Le stockage et la protection des clés privées ainsi que les respects des droits accordés sur chacun des objets contenus dans la carte sont assurés par la puce électronique de la carte CPx.

Tableau 105 : Sécurité : Certificats et clés privées

18.3 Common Vulnerabilities and Exposures (CVE)

La Cryptolib CPS ne fait l'objet d'aucune CVE référencée en date d'édition de ce document.

18.4 Code porteur

18.4.1 Saisie des codes porteur et déblocage

#	Cryptolib CPS : Saisie du code porteur	
1	Le nombre de saisies du code porteur est limité à 3 essais. Passés 3 essais faux, il faut débloquer la carte à l'aide du code de déblocage. Le nombre de déblocages est lui aussi limité, la carte est alors inutilisable (du moins, les parties protégées par code porteur).	
2	Dans tous les cas, la saisie du code porteur est masquée. Le nombre de tentatives restantes est indiqué. La raison d'un code porteur faux n'est pas complètement précisée sciemment afin de ne pas divulguer trop d'informations à un éventuel attaquant.	
3	Les mêmes remarques sont valables pour le code de déblocage.	
4	**Cryptolib CPS v4**	La saisie du code porteur est assurée par la partie PKCS#11 de la Cryptolib CPS (voir architecture)
	Cryptolib CPS v5	La saisie du code porteur est assurée par la partie CSP de la Cryptolib CPS (Windows, voir architecture)
5	**Cryptolib CPS v4**	La validité du code porteur est partagée entre toutes les applications clientes.
	Cryptolib CPS v5	Le code porteur doit être saisi dans chaque contexte applicatif.

Tableau 106 : Cryptolib CPS : Saisie du code porteur

18.4.2 Déblocage du code porteur

3 procédures permettent de débloquer le code porteur d'une carte CPx :

#	Description
1	L'outil CPS-Gestion permet au porteur de débloquer sa carte CPx en entrant le code de déblocage fourni avec le courrier d'envoi de la carte CPx (mailer).
2	Le Support CPS Info Service (0 825 85 2000) propose une aide 24/24 7/7 au déblocage.
3	L'ASIP Santé propose un outil de déblocage en ligne à l'adresse : http://esante.gouv.fr/services/espace-cps/assistance/deblocage-de-carte

Tableau 107 : Cryptolib CPS : Procédures de déblocage de la carte CPx

18.4.3 Changement du code porteur

L'utilisateur peut changer le code porteur de sa carte CPx.

L'utilisateur peut donc spécifier un code porteur qu'il retiendra plus facilement que celui fourni par l'ASIP Santé.

Cette fonctionnalité permet aussi de changer un code porteur que l'utilisateur juge compromis.

L'ASIP Santé n'est pas informé du nouveau code porteur en cas de changement par l'utilisateur. En cas de recouvrement de code porteur par exemple, le « mailer » contiendra toujours l'ancien code porteur.

Tableau 108 : Cryptolib CPS : Avertissement changement de code porteur et procédure de recouvrement

18.4.4 Cache des codes porteur et déblocage

La Cryptolib CPS ne maintient pas de cache du code porteur : le code porteur saisi est transmis à la carte et n'est pas conservé.

La carte CPx gère en interne un état « code porteur présenté » (et non pas une valeur de code, cf. ISO 7816 et normes IAS-ECC).

Cet état est consultable par la Cryptolib CPS et peut donc être « remonté » aux applications.

Les mêmes remarques sont valables pour le code de déblocage.

18.5 Cache de fichiers carte

<table>
<tr><th>#</th><th colspan="3">Cryptolib CPS : Cache de fichier carte</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">Cryptolib CPS v4</td><td colspan="2">Seuls les certificats de la carte CPx sont mis en cache dans le fichier ccert.bin.
L'ensemble des certificats correspondant aux cartes lues sur le poste se retrouve dans cet unique fichier.
Ces données ne sont pas confidentielles.
Le fichier ccert.bin doit être accessible en lecture/écriture.</td></tr>
<tr><td>ccert.bin</td><td>%ALLUSERSPROFILE%\santesocial\cps\coffre\ccert.bin</td></tr>
<tr><td rowspan="4">2</td><td rowspan="4">Cryptolib CPS v5</td><td colspan="2">La Cryptolib CPS v5 maintient un cache des fichiers des cartes CPx lues sur le poste.
Ce cache prend la forme d'un répertoire cache\ qui contient autant de fichiers que le poste n'a vu de cartes et de fichiers par carte.
La Cryptolib CPS v5 implémente un mécanisme de recouvrement du cache au cas où il serait corrompu.
Les fichiers du cache sont sécurisés, propres à une carte donnée et à l'environnement qui les a créés.
Le répertoire cache\ doit être accessible en lecture/écriture.</td></tr>
<tr><td rowspan="3">Cache\</td><td>%ALLUSERSPROFILE%\santesocial\cps\cache\</td></tr>
<tr><td>%USERPOFILE%\AppData\Local\Microsoft\Windows\INetCache\Virtualized\C\ProgramData\santesocial\cps\cache\</td></tr>
<tr><td>Sous Win8 avec EPM activé :

%PUBLIC%\AppData\santesocial\cps\cache\</td></tr>
</table>

Tableau 109 : Cryptolib CPS : Cache de fichier carte

18.6 Logs de la Cryptolib CPS

Lorsque les traces de la Cryptolib CPS sont activées, aucune donnée sensible n'est inscrite dans les logs.

18.7 Signature numérique

18.7.1 Performances

Les performances de l'opération de signature sont liées à l'efficacité du l'algorithme de hachage qui précède la signature effective.

<table>
<tr><td>PC/SC, PKCS#11, CSP</td><td colspan="2">L'intégrateur doit choisir la taille du buffer de données soumis au hash. Idéalement, cette taille doit être paramétrable.</td></tr>
<tr><td rowspan="3">Langages managés</td><td colspan="2">Microsoft et Oracle font réaliser le hash par leurs propres implémentations, sensées garantir des performances optimales.</td></tr>
<tr><td>Microsoft</td><td>Par défaut, le hash est calculé par le provider Microsoft Enhanced RSA and AES Cryptographic Provider (type 24, RSA Full and AES, sous Vista+).
Avec les classes .NET, la taille de buffer des données soumises au CSP est de 4096 bytes et non paramétrable, ce qui est à mettre en relation avec la taille moyenne des données que l'application est sensée signer.</td></tr>
<tr><td>Oracle</td><td>Par défaut, le provider sunMSCAPI délègue le calcul du SHA-1 au provider "SUN".</td></tr>
</table>

Tableau 110 : Cryptolib CPS : Performances en signature numérique

18.7.2 Sécurité

Le RGS recommande que l'opération de signature effective soit effectuée en faisant calculer le dernier tour de hash à la carte pour signature. La carte CPS3 est conforme à cette recommandation : le volet CPS3 et la librairie PKCS#11 de la CPS3 rejettent l'opération de signature de hash pré calculé.

<table>
<tr><td rowspan="2">PC/SC, PKCS#11</td><td>Volet 2Ter</td><td>Le hash peut être calculé en dehors de la carte et soumis à la carte pour signature.</td></tr>
<tr><td>Volet CPS3</td><td>Conformément au RGS, la signature est obligatoirement faite en faisant calculer le dernier tour de hash à la carte pour signature. Le présent document parle par la suite de « signature IAS-ECC » pour désigner cette fonctionnalité.</td></tr>
<tr><td>CSP / Langages managés</td><td colspan="2">Les 2 comportements sont possibles, paramétrés par la valeur de Sign_Hash.</td></tr>
</table>

Tableau 111 : Cryptolib CPS : signature numérique et RGS

18.8 Sans contact

Le volet sans contact de la carte CPS3 tient compte des considérations de sécurités induites par le « sans fil ». En particulier, les données exposées en sans contact peuvent être lues à l'insu du porteur de la carte (cas d'un « porteur » de lecteur de carte sans contact dans un lieu public par exemple).

Le volet sans contact de la carte CPS3 a donc fait l'objet d'un dépôt de dossier CNIL qui encadre le type d'informations exposées. Dans ce contexte, les données accessibles en sans contact sont des données non nominatives et non reliables au porteur de la carte :

- Le certificat X.509 sans contact est un certificat « technique » non nominatif
- Il n'existe aucun fichier de correspondance entre numéro de série sans contact et carte physique

18.9 Antivirus

La Cryptolib CPS n'est pas testée au regard des antivirus disponibles sur le marché.

Aucune anomalie relative à des dysfonctionnements de la Cryptolib CPS avec des antivirus n'est actuellement connue.

Certains antivirus apportent un fonctionnement dit « en bac à sable » (« sandbox ») qui leur permet d'isoler un exécutable qu'ils voient s'exécuter pour la première fois sur le poste. Ces antivirus affichent alors des messages supplémentaires à l'utilisateur lorsque les .MSI s'installent ou que les exécutables sont actifs. L'ergonomie de l'installation ou de l'exécution des services peut ainsi être altérée. Un paramétrage supplémentaire lié à l'antivirus en question peut être nécessaire (création des règles d'acceptation d'exécution permanente par exemple, voir manuel de l'antivirus).

Désactivation de l'antivirus	Aucune désactivation d'antivirus n'est à priori requise. Cette opération, si elle devait être réalisée, doit se faire en toute connaissance de cause et d'effet. En particulier, il est alors préférable de quitter toutes les applications et de réaliser les tâches prévues « hors ligne ». Consulter un professionnel en cas de doute.

18.10 Pare-feu

La Cryptolib CPS n'est pas testée au regard des pare-feux disponibles sur le marché.

Aucune anomalie relative à des dysfonctionnements de la Cryptolib CPS avec des pare-feu n'est actuellement connue. Le pare-feu doit être configuré de sorte que les prérequis « internet » cités plus haut soient remplis.

Désactivation du pare-feu	Aucune désactivation de pare-feu n'est à priori requise. Cette opération, si elle devait être réalisée, doit se faire en toute connaissance de cause et d'effet. En particulier, il est alors préférable de quitter toutes les applications et de réaliser les tâches prévues « hors ligne ». Consulter un professionnel en cas de doute.

18.11 Considérations de sécurité sous Microsoft Windows

18.11.1 Gestion des fichiers .MSI

Pour des raisons de sécurité, il est recommandé de ne pas conserver les .MSI sur les machines de production.

A défaut :

- Les fichiers peuvent être renommés afin de « casser » l'association .MSI <-> « msiexec »
- Les droits d'exécution accordés sur les .MSI aux utilisateurs du système doivent être maitrisés.
- Le répertoire de stockage des .MSI doit être protégé par des règles d'accès précis (lecture/écriture/exécution pour les administrateurs)

18.11.2 Comptes utilisateur

La Cryptolib CPS ne nécessite pas de création préalable de compte utilisateur particulier.

Elle ne nécessite pas non plus de modification des comptes existants sur le poste.

L'installeur de la Cryptolib CPS requiert une élévation de privilèges. Le compte administrateur par défaut peut être utilisé (mot de passe du compte ou présence de l'administrateur du poste requis).

18.11.3 Services

Afin d'installer des .MSI, le service **msiserver** doit être lancé (il l'est par défaut, il peut avoir été arrêté par mesure de sécurité).

L'installeur de la Cryptolib CPS s'assure que le service **SCardSvr** se lance automatiquement. **SCardSvr** est indispensable avec les lecteurs PC/SC.

Le service de propagation du certificat **CertPropSvc** n'est pas indispensable si le CCM est utilisé.

18.11.4 Démarrage

L'installeur de la Cryptolib CPS positionne l'exécutable CCM.exe pour qu'il se lance au démarrage des sessions utilisateur.

Il le fait en installant un raccourci dans le menu démarrer de « all users ».

Il ne modifie en aucun cas les clés « «run » ou « shell » de Windows.

18.13 Considérations de sécurité sous Linux

18.13.1 Comptes utilisateurs

Distribution	Groupe	Commentaire
Fedora	dialout	Le compte utilisant un lecteur PSS doit être ajouté au group dialout : `usermod $USER -G dialout`

Tableau 113 : Linux : Comptes

18.13.2 Droits

Dossier d'installation	Fichier	Droit d'accès	Remarques
/usr/lib/	libcps3_pkcs11_lux.so	lrwxrwxrwx	Lien symbolique
	libcps_pkcs11_lux.so	lrwxrwxrwx	Lien symbolique
/usr/bin/	cpgeslux	lrwxrwxrwx	Lien symbolique
/opt/santesocial/CPS/lib/	libcps3_pkcs11_lux.so	rwxr_xr_x	Librairie PKCS11 CPS3
/opt/santesocial/CPS/bin/	cpgeslux	rwxr_xr_x	CPS-Gestion
/etc/opt/santesocial/CPS/	DICO-FR.GIP	rw_r__r__	Dictionnaire
	cps_pkcs11_safe.ini	rw_r__r__	Fichier de configuration de la librairie PKCS#11 CPS2Ter
	cps3_pkcs11.conf	rw_r__r__	Fichier de configuration de la librairie PKCS#11 CPS3
/etc/opt/santesocial/CPS/Coffre/	*.cer	rw_r__r__	Certificats d'autorités
/usr/local/galss/	libcps_pkcs11_lux.so	rwxr_xr_x	Librairie PKCS11 CPS2ter
	cpgeslux.old	rwxr_xr_x	Application de Gestion de la CPS2ter
	libcpslux.so	rwxr_xr_x	Librairie CPS
	libcptablux.so	rwxr_xr_x	Module de gestion du dictionnaire
	libsscaslux.so	rwxr_xr_x	Couche d'Abstraction Système CPS
/etc/ld.so.conf.d/	Cryptolib.conf	rw_r__r__	Fichier de configuration pour le chargement des librairies présentes dans le répertoire /usr/local/galss

Tableau 114 : Linux : Droits accordés par défaut

19 Architecture

19.1 Principales API Cryptographiques du poste de travail

19.1.1 CryptoAPI (ou CAPI) / CSP

CAPI est le sigle de Cryptographic Application Program Interface.

CAPI est une API développée par Microsoft qui définit un jeu de fonctions cryptographiques utilisables par les applications Windows. Un module logiciel qui implémente ces fonctions se nomme un CSP pour "Cryptographic Service Provider".

Un CSP doit être signé par Microsoft ou par Authenticode (cf. KBs en Annexe) avant d'être utilisable.

19.1.2 Common Data Security Architecture (ou CDSA) / Tokend

CDSA est une architecture développée par Apple qui définit un jeu de fonctions cryptographiques utilisables par les applications Macintosh.

Un module logiciel qui implémente ces fonctions se nomme un Tokend.

19.1.3 PKCS#11

PKCS est le sigle de Public Key Cryptography Standards, ensemble de standards de cryptographie à clé publique initialement édités par RSA Labs.

PKCS#11 définit un jeu de fonctions cryptographiques utilisables par les applications locales. Un module logiciel qui offre des fonctions PKCS#11 se nomme **Cryptoki**.

Le standard PKCS#11 évolue désormais sous l'égide de OASIS (version 2.3 et ultérieures).

19.2 Architecture du poste de travail de santé

La Cryptolib CPS est le nom donné au composant logiciel distribué par l'ASIP Santé

- répondant aux trois interfaces CSP/Tokend/PKCS#11
- utilisant les cartes CPx

Ce composant présente donc les trois interfaces :

- La bibliothèque CryptoAPI: CSP-CPS (environnements Windows).
- Le Tokend CDSA : GIP-CPS.tokend (environnements Macintosh).
- La bibliothèque PKCS#11 : PKCS#11-CPS (environnements Windows, Mac OS X et Linux).

Ces trois composants, **Cryptolib CPS** (constitué des trois bibliothèques **CSP-CPS**, **GIP-CPS.tokend**, et **PKCS#11-CPS**), **API-CPS** et **GALSS** s'articulent suivant ce schéma de principe :

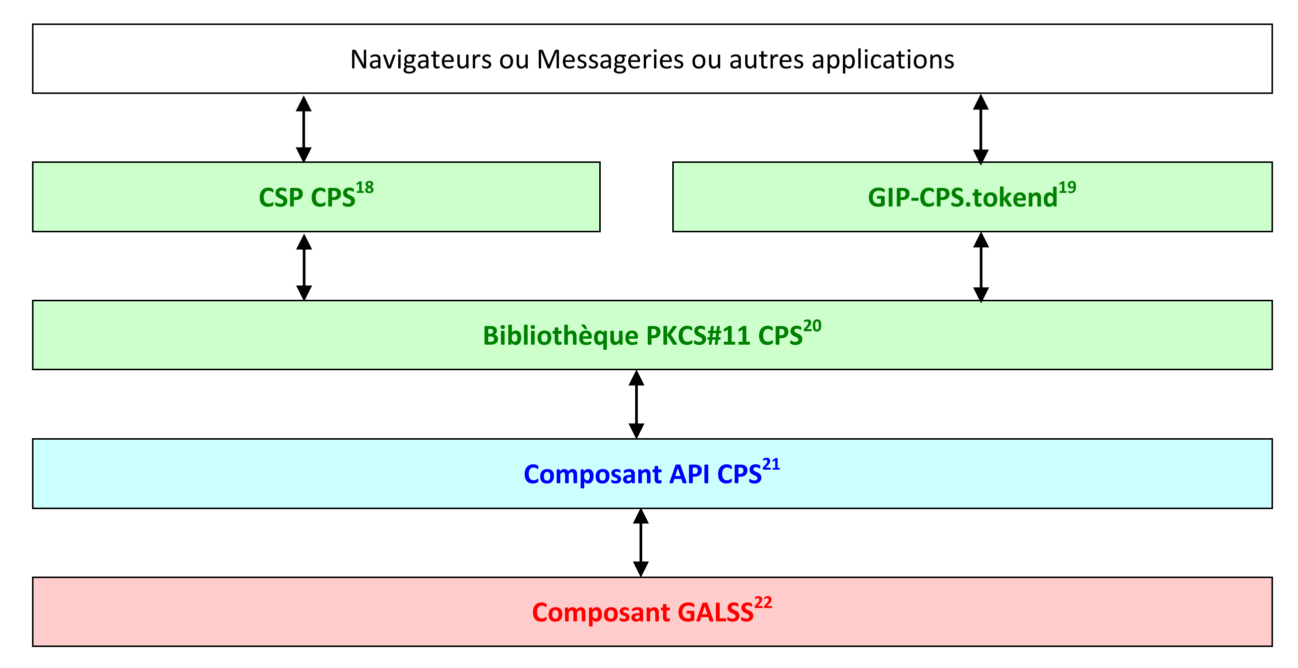


Figure 104 : Architecture : Architecture du poste de travail de Santé

[18] Le CSP n'existe que pour les OS Windows.

[19] La bibliothèque GIP-CPS.tokend n'existe que pour les OS Macintosh.

[20] La bibliothèque PKCS#11 CPS est implémentée pour les trois OS : Windows, Mac OS X et Linux.

[21] Le composant API CPS est aussi utilisé directement par les applications accédant à la carte CPx (agent RSS, lecture Vitale, OSM, etc…). **Il est aujourd'hui déprécié en faveur de la nouvelle API PKCS#11 introduite par la Cryptolib CPS v5 (cf. [16])**

[22] Le composant GALSS est aussi utilisé par les applications de gestion des FSE (GIE SESAM-Vitale).

19.3 Spécificités de l'architecture Mac OS X

CDSA (Common Data Security Architecture) est un standard d'architecture de sécurité conçu par Intel et implémenté par Apple dans son système d'exploitation Mac OS X.

Le cœur de CDSA est le module « serveur de sécurité » (SecurityD), qui s'appuie à la fois

1. sur le protocole PC/SC (démon PCSCD) pour la gestion des lecteurs
2. sur des modules appelés Tokend fournis par chaque organisme émetteur de cartes à puces

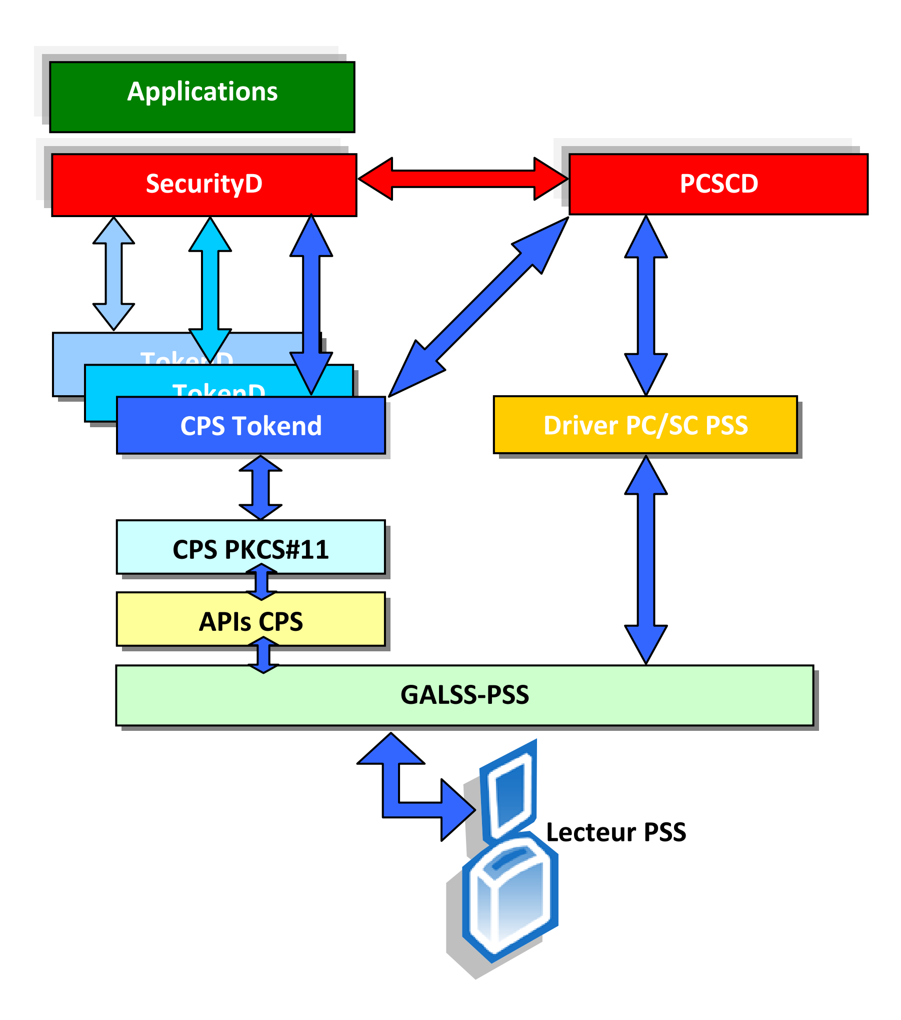


Figure 105 : Architecture : Tokend

Le serveur de sécurité détecte l'insertion d'une carte dans un lecteur avec l'aide du gestionnaire de ressources PC/SC.

Le serveur de sécurité interroge alors les différents Tokend existant afin d'identifier celui qui gère la carte insérée.

Le Tokend identifié est chargé. Le système est en mesure d'effectuer d'utiliser la carte en lui demandant d'effectuer des opérations cryptographiques et en y récupérant des objets (certificats, clés publiques…).

Certaines applications Macintosh (ex : le navigateur Safari) ne se basent que sur cette architecture.

Les bibliothèques cryptographiques de l'ASIP Santé doivent donc s'intégrer dans CDSA pour que ces applications soient capables de fonctionner avec la carte CPS.

Pour cela, l'ASIP fournit 2 composants :

- le **CPS Tokend** : module au standard Tokend d'Apple, qui permet de s'interfacer dans CDSA afin d'offrir le support de la carte CPS comme module cryptographique. Le Tokend utilise l'architecture PC/SC pour la détection des cartes CPS et le module CPS PKCS#11 pour réaliser les opérations cryptographiques.

Le module **CPS Tokend** est suffisant pour faire fonctionner le système avec un lecteur PC/SC et une carte CPS.

Un **driver PC/SC** pour les lecteurs de type PSS (lecteurs série: bifente S-V et monofente NF-CPS) est fourni en complément afin de pouvoir utiliser la carte CPS au sein de cette architecture:

- le **driver PC/SC PSS** : c'est un driver simplifié qui permet d'intégrer les lecteurs PSS dans l'architecture PC/SC, au niveau du démon PCSCD. Il permet de détecter la présence d'une carte CPS dans les lecteurs de type RS232 (Série), en utilisant la couche GALSS-PSS. Son rôle est donc de prendre en charge les lecteurs de type PSS, qui pourront ainsi fonctionner dans l'environnement CDSA.

La totalité des lecteurs susceptibles d'utiliser la carte CPS est ainsi couverte.

19.4 Intégration avec l'API de lecture SESAM-Vitale

Cette API apporte les fichiers suivants :

#	Fichier	Description
1	api_lec.dll	
2	api_lec.ini	
3	pdt-cdc-011.csv	
4	sedica.ini	
5	tablebin.hab	
6	tablebin.lec	

Tableau 115 : API de lecture SESAM-Vitale : Composants

DMP	Dans le cadre de l'AW PS DMP, l'API de lecture Vitale est installée dans : %USERPROFILE%\Application Data\santesocial\DMP\

Tableau 116 : API de lecture SESAM-Vitale : Exemple de répertoire d'installation : DMP

Les droits de lecture et d'exécution ont été donnés à tous les utilisateurs sur le répertoire d'installation.

19.4.1 Configuration de l'API de lecture SESAM-Vitale pour l'AW PS DMP

Deux fichiers de configuration **api_lec.ini** et **sedica.ini** sont utilisés par l'API de lecture.

Ces deux fichiers doivent être correctement renseignés en fonction de la configuration du poste.

19.4.1.1 Poste utilisant un lecteur bi-fentes

```
[CONFIG]
NbLecteur=2
Mode=NORMAL
[LECTEUR01]
TypeLecteur=SEDGAPSS
NumCoupleur=1
NomRessource=TRANSPA1

[LECTEUR02]
TypeLecteur=SEDGAPSS
NumCoupleur=1
NomRessource=TRANSPA2
```

Tableau 117 : API de lecture SESAM-Vitale : lecteur bi-fentes : Contenu du fichier sedica.ini

```
[Mode]
Mode = CPS_EN_LIGNE

[Timer]
TimerInactivite = 60
TimerControle = 120
```

Tableau 118 : API de lecture SESAM-Vitale : lecteur bi-fentes : Contenu du fichier api_lec.ini

19.4.1.2 Poste utilisant deux lecteurs PC/SC

```
[CONFIG]
NbLecteur=2
Mode=NORMAL

[LECTEUR01]
TypeLecteur=SEDGAPSS
NumCoupleur=1
NomRessource=TRANSPA1

[LECTEUR02]
TypeLecteur=SEDGAPSS
NumCoupleur=2
NomRessource=TRANSPA2
```

Tableau 119 : API de lecture SESAM-Vitale : deux lecteurs PC/SC: Contenu du fichier sedica.ini

```
[Mode]
Mode = CPS_EN_LIGNE

[Timer]
TimerInactivite = 60
TimerControle = 120
```

Tableau 120 : API de lecture SESAM-Vitale : deux lecteurs PC/SC: Contenu du fichier api_lec.ini

19.4.2 Configuration du fichier galss.ini pour l'API de lecture SESAM-Vitale

L'API de lecture SESAM-Vitale a besoin d'une configuration particulière du fichier galss.ini.

- Pour la ressource CPS, l'alias TRANSPA1 doit être déclaré (c'est-à-dire NbAlias=1 ou plus, et NomAliasZ=TRANSPA1 avec Z inférieur ou égal à NbAlias)

- Pour la ressource Vitale, l'alias TRANSPA2 doit être déclaré (c'est-à-dire NbAlias=1 ou plus, et NomAliasZ=TRANSPA2 avec Z inférieur ou égal à NbAlias)

Important : L'installeur porté par l'applet Java de l'AW PS DMP gère uniquement les 2 cas suivants pour la configuration lecteur :

- 1 lecteur bi-fente connecté au poste de travail
- 2 lecteurs mono-fente PC/SC connectés au poste de travail

```
[CANAL1.PAD1.LAD1]
LAD=1
NomLAD=CPS
NbAlias=1
NomAlias1=TRANSPA1

[CANAL1.PAD1.LAD3]
LAD=2
NomLAD=Vitale
NbAlias=1
NomAlias1=TRANSPA2
```

Tableau 121 : API de lecture SESAM-Vitale : Exemple de fichier galss.ini pour un poste utilisant un lecteur bi-fente

```
[CANAL1.PAD1.LAD1]
LAD=1
NomLAD=CPS
NbAlias=1
NomAlias1=TRANSPA1

[CANAL2.PAD1.LAD1]
LAD=1
NomLAD=Vitale
NbAlias=1
NomAlias1=TRANSPA2
```

Tableau 122 : API de lecture SESAM-Vitale : Exemple de fichier galss.ini pour un poste utilisant deux lecteurs PC/SC

19.5 Intégration via les APIs logicielles

L'intégration logicielle avec la carte CPx et la Cryptolib CPS peut se faire aux différents « étages » de l'architecture présentée plus haut.

19.5.1 PC/SC

L'intégration via une communication directe avec la carte CPx est possible à partir des cartes CPS3.

Les documents de référence, nécessitant la signature d'une convention, pour effectuer une intégration logicielle au niveau PC/SC sont les suivants.

Cryptolib CPS v5	**[8]**	Procédure de concessions des spécifications de la carte CPS3
	[15]	Carte CPS - Guide de référence de la carte CPS3

Tableau 123 : Cryptolib CPS v5 : documents de référence pour intégration PC/SC

Accès concurrents	Les accès concurrents sont gérés via le Ressource manager PC/SC, avec un mode partagé ou un mode exclusif	
	L'utilisation du mode partagé est préconisée, plusieurs applications pouvant cohabiter sur un même poste.	
Recommandations	Recommandé aux intégrateurs connaissant déjà préalablement bien la carte à puce, le standard PC/SC, les normes ISO 7816 et les principaux standards cryptographiques.	
	Recommandé pour les intégrations de la CPx dans du logiciel embarqué	
	Recommandé pour les solutions prévoyant une gestion fine des erreurs et des événements lecteurs et cartes (arrachages / insertions lecteurs et/ou cartes)	
	Recommandé pour les solutions cherchant à optimiser la présentation des codes porteurs (PIN et PUK)	
	Recommandé pour les solutions cherchant la conformité avec le RGS (SHA256 et signature IAS-ECC)	
Langage	C / C++	
	Java 6+	via javax.smartcardio
	C# / .NET	via P/Invoke
Plates-formes	Windows (32b et 64b), Linux (32b) et Mac OS X (32b et 64b)	

Tableau 124 : Cryptolib CPS v5 : recommandations pour intégration PC/SC

19.5.2 API CPS

L'**API CPS**, ensemble de fonctions de haut niveau permettant d'accéder aux informations de la carte, est **dépréciée** (« deprecated »).

Les éditeurs pourront se tourner progressivement vers la nouvelle API PKCS#11 de la Cryptolib CPS v5.

19.5.3 PKCS#11

La Cryptolib CPS apporte un composant Cryptoki pour Windows, Mac OS X et Linux. Il est donc possible d'intégrer la CPS via l'API PKCS#11.

Les documents de référence pour effectuer une intégration logicielle au niveau PKCS#11 sont les suivants:

Cryptolib CPS v5	**[12]**	Manuel de programmation de la Cryptolib CPS v5
	[13]	Documentation programme d'exemple de la Cryptolib CPS v5
	[14]	Spécifications externes PKCS#11 de la Cryptolib CPS v5
	[16]	Impacts de la migration Cryptolib CPS v4 vers la Cryptolib CPS v5

Tableau 125 : Cryptolib CPS v5 : documents de référence pour intégration PKCS#11

Accès concurrents	Les accès concurrents sont gérés via un gestionnaire de sessions	
Recommandations	Fortement recommandée du fait de la large diffusion et adoption	
	Recommandé pour les solutions prévoyant une gestion fine des erreurs et des événements lecteurs et cartes	
	Recommandé pour les solutions cherchant la conformité avec le RGS (SHA256 et signature IAS-ECC)	
Langage	C / C++	
	Java	via JNI
	C# / .NET	via P/Invoke
Plates-formes	Windows (32b et 64b), Linux (32b) et Mac OS X (32b et 64b)	

Tableau 126 : Cryptolib CPS v5 : recommandations pour intégration PKCS#11

Cryptolib CPS v5	Les implémentations PKCS#11 de la Cryptolib CPS v4 et de la Cryptolib CPS v5 sont légèrement différentes. Il est toutefois possible d'implémenter une solution indépendante du PKCS#11 Cryptolib CPS v4 et PKCS#11 Cryptolib CPS v5, fonctionnant pour les 2 .DLL PKCS#11 sans tomber dans le « if / then / else » (voir **[16]** Impacts de la migration Cryptolib CPS v4 vers la Cryptolib CPS v5 et spécifications PKCS#11[23])

Tableau 127 : Cryptolib CPS: Recommandation d'utilisation de l'API PKCS#11

[23] Nécessite un compte sur integrateurs-cps, s'adresser à editeurs@asipsante.fr

19.5.4 CSP

La Cryptolib CPS apporte une DLL CSP pour Windows. Il est donc possible d'intégrer la CPS via l'API CryptoAPI de Microsoft.

L'intégration au niveau CSP est recommandée sous Windows, cette interface étant largement diffusée et adoptée.

Cryptolib CPS v5	Using Cryptography
	Using Certificates

Tableau 128 : Cryptolib CPS v5 : documents de référence pour intégration CSP

Accès concurrents	Les accès concurrents sont gérés via l'acquisition d'un contexte cryptographique	
Recommandations	Pour les solutions fortement intégrées aux infrastructures Microsoft	
Langage	C / C++	
	Java	via JNI
		via JCA/sunMSCAPI
	C# / .NET	via P/Invoke
Plates-formes	Windows (32b et 64b)	

Tableau 129 : Cryptolib CPS v5 : recommandations pour intégration CSP

Cryptolib CPS	La Cryptolib CPS offre un large choix de scénarios d'intégration logicielle avec la carte CPx.

Tableau 130 : Cryptolib CPS: Remarques choix de scénarios d'intégration de la carte CPx

19.6 Intégration de la Cryptolib CPS avec les langages managés

Java / JRE et C# / .NET apportent des bibliothèques cryptographiques qui permettent d'exploiter rapidement la carte CPx et la Cryptolib CPS (moins de 10 lignes de code effectif).

19.6.1 Java

<table>
<tr><th>Niveau</th><th colspan="4">Possibilités d'intégration de la CPx /de la Cryptolib CPS avec Java</th></tr>
<tr><td>au niveau PKCS#11</td><td>Toute plate-forme (32b et 64b)</td><td>via JNI</td><td colspan="2">wrapper IAIK par exemple sous licence IAIK</td></tr>
<tr><td rowspan="5">au niveau JCA/JCE</td><td colspan="4">L'intégration au niveau JCA/JCE est possible malgré une limitation structurelle de l'architecture Java</td></tr>
<tr><td rowspan="2">Toute plate-forme (32b et 64b)</td><td rowspan="2">via provider JCA/JCE pour PKCS#11</td><td>v4</td><td rowspan="2">- SunPKCS11 (fourni avec la JVM)
- PKCS#11 de IAIK par exemple (commercial)</td></tr>
<tr><td>v5</td></tr>
<tr><td rowspan="2">Windows (32b et 64b)</td><td rowspan="2">via provider JCA/JCE sunMSCAPI</td><td>v4</td><td>dans tous les cas</td></tr>
<tr><td>v5</td><td>si l'option Sign_Hash est activée (valeur 1, appliquée par défaut), uniquement</td></tr>
</table>

Tableau 131 : Niveau d'intégration de la Cryptolib CPS avec Java

```
import java.security.KeyStore;
import java.security.KeyStoreSpi;
import java.security.PrivateKey;
import java.security.Signature;
import java.security.cert.X509Certificate;

[...]

//ASIP: données à signer:
final byte[] data = [...];

//ASIP: initialisation du CSP:
final KeyStore ks = KeyStore.getInstance("Windows-MY", "SunMSCAPI");
ks.load(null, null);

//ASIP: on obtient la référence sur la clé de signature:
final PrivateKey sigKey = findSignatureKey(ks);

//ASIP: initialisation de l'algorithme de cryptographie:
final Signature rsa = Signature.getInstance("SHA1withRSA");
rsa.initSign(sigKey);
rsa.update(data, 0, data.length);

//ASIP: calcul de la signature numérique:
byte[] signature = rsa.sign();

//ASIP: affichage de la signature numérique:
System.out.println("signature: " + toHexString(signature));
```

Tableau 132 : Java/JCA: exemple de code de signature numérique avec la CPx et l'API de cryptographie du JRE (niveau CSP sous Microsoft Windows)

```
import java.security.Provider;

import java.security.KeyStore;
import java.security.KeyStoreSpi;
import java.security.PrivateKey;
import java.security.Signature;
import java.security.cert.X509Certificate;

[...]

//ASIP: données à signer:
final byte[] data = [...];

//ASIP: initialisation du PKCS#11:
final Provider p = Security.getProvider("SunPKCS11-CPS");
if (p == null) {
    final StringBuilder cardConfig = new StringBuilder();
    cardConfig.append("name = CPS\n");
    //ASIP: voir partie PKCS#11 pour localisation du module ASIP Santé / PKCS#11:
    cardConfig.append("library = " + ToolsImpl.findPkcs11Module());
    final InputStream is = new ByteArrayInputStream(cardConfig.toString().getBytes());
    final Provider securityProvider = new sun.security.pkcs11.SunPKCS11(is);
    Security.addProvider(securityProvider);
}

final KeyStore ks = KeyStore.getInstance("PKCS11");
ks.load(null, PWD);

//ASIP: le reste est strictement identique au scénario d'intégration
//au niveau CSP sous Windows : on bascule sur les APIs JCA/JCE :

//ASIP: on obtient la référence sur la clé de signature:
final PrivateKey sigKey = findSignatureKey(ks);

//ASIP: initialisation de l'algorithme de cryptographie:
final Signature rsa = Signature.getInstance("SHA1withRSA");
rsa.initSign(sigKey);
rsa.update(data, 0, data.length);

//ASIP: calcul de la signature numérique:
byte[] signature = rsa.sign();

//ASIP: affichage de la signature numérique:
System.out.println("signature: " + toHexString(signature));
```

Tableau 133 : Java/JCA: exemple de code de signature numérique avec la CPx et l'API de cryptographie du JRE (niveau PKCS#11 avec Provider Oracle)

19.6.2 .NET

L'intégration de la CPx avec le framework .NET est possible.

<table>
<tr><th>Niveau</th><th colspan="4">Possibilités d'intégration de la CPx avec le framework .NET</th></tr>
<tr><td>au niveau PKCS#11</td><td>Windows (32b et 64b)</td><td>via les APIs PKCS#11 et P/Invoke</td><td colspan="2">pkcs11interop par exemple sous licence AGPL</td></tr>
<tr><td rowspan="4">au niveau CSP</td><td rowspan="4">Windows (32b et 64b)</td><td rowspan="2">via les APIs CSP et P/Invoke</td><td>v4</td><td rowspan="2">wrapper IDRIX par exemple sans aucune licence</td></tr>
<tr><td>v5</td></tr>
<tr><td rowspan="2">via les packages de cryptographie du framework .NET</td><td>v4</td><td>dans tous les cas</td></tr>
<tr><td>v5</td><td>si l'option Sign_Hash est activée (valeur 1, appliquée par défaut), uniquement</td></tr>
</table>

Tableau 134 : Niveau d'intégration de la Cryptolib CPS avec le framework .NET

```
using System.Security.Cryptography;

[...]

//ASIP: données à signer:
byte[] data = [...];

//ASIP: initialisation du CSP:
//Type du CSP: 1
//1 = PROV_RSA_FULL (le type de CSP par défaut sous Win7 est maintenant PROV_RSA_AES (24))
int CSP_TYPE = 1;
//Nom du CSP: "ASIP Sante Cryptographic Provider", déclaré en BdR par le .MSI d'installation
string CSP_NAME = "ASIP Sante Cryptographic Provider";
//Algorithme de hash: SHA1, pas de SHA256 avec PROV_RSA_FULL bien que la carte en soit capable:
string HASH_ALG_NAME = "SHA1";
string CIPH_ALG_NAME = "RSA";

CspParameters csp = new CspParameters(CSP_TYPE, CSP_NAME);
csp.Flags = CspProviderFlags.UseDefaultKeyContainer;
csp.KeyNumber = (int) KeyNumber.Signature;
Object[] argsArray = new Object[] { csp };

//ASIP: initialisation des algorithmes cryptographiques:
RSACryptoServiceProvider rsa =
    (RSACryptoServiceProvider) CryptoConfig.CreateFromName(CIPH_ALG_NAME, argsArray);
HashAlgorithm hashAlg = (HashAlgorithm) CryptoConfig.CreateFromName(HASH_ALG_NAME);

//ASIP: calcul du hash:
byte[] hash = hashAlg.ComputeHash(data);
//ASIP: calcul de la signature numérique:
byte[] signature = rsa.SignHash(hash, HASH_ALG_NAME);

//ASIP: affichage de la signature numérique:
Console.WriteLine("signature: " + BitConverter.ToString(signature).Replace("-", " "));
```

Tableau 135 : .NET/C# : exemple de code de signature numérique avec la CPx et l'API de cryptographie du framework .NET

Cryptolib CPS	**L'intégration de la carte CPx avec des langages et des frameworks de hauts niveaux est particulièrement facile et directe.**

Tableau 136 : Cryptolib CPS: Remarques complexités intégration carte CPx

```
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;

[...]

//ASIP: par rapport au code précédent, une autre méthode pour récupérer
//ASIP: une référence sur un objet de type RSACryptoServiceProvider:

X509Certificate2 cert = null;
Try {
    X509Store store = new X509Store(StoreName.My, StoreLocation.CurrentUser);
    store.Open(OpenFlags.ReadOnly | OpenFlags.OpenExistingOnly);

    X509Certificate2Collection collection = (X509Certificate2Collection)store.Certificates;

    //ASIP: sélection du certificat de signature ASIP Santé sur la base de l'examen des Usages :
    X509Certificate2Collection fcollection = (X509Certificate2Collection)
        collection.Find(X509FindType.FindByTimeValid, DateTime.Now, false)
                  .Find(X509FindType.FindByExtension, new X509KeyUsageExtension().Oid.Value, false)
                  .Find(X509FindType.FindByKeyUsage, X509KeyUsageFlags.NonRepudiation, false)
                  .Find(X509FindType.FindByKeyUsage, X509KeyUsageFlags.DigitalSignature, false)
                  .Find(X509FindType.FindByIssuerName, "GIP-CPS", false);

    if (fcollection != null && fcollection.Count == 1) {
        cert = fcollection[0];
        if (cert.HasPrivateKey == false) {
            cert = null;
        }
    }
    store.Close();
} catch (Exception) {
    //ASIP: gestion des exceptions :
    [...]
}
RSACryptoServiceProvider rsa = (RSACryptoServiceProvider)cert.PrivateKey;

//ASIP: suite de la signature électronique:
[...]
```

Tableau 137 : .NET/C# : exemple de code de sélection du certificat ASIP Santé de signature numérique avec la CPx et l'API de cryptographie du framework .NET



19.7 Matrice d'intégration

La Cryptolib CPS permet de s'interfacer logiciellement avec la carte CPx à différents niveaux, sur différentes plates-formes et dans différents langages.

Le choix de l'interfaçage doit être fait en fonction :

1. des compétences et de l'expertise disponible
2. de l'expression de besoin initiale et des fonctionnalités à implémenter

#	Domaine	Section	PC/SC	PKCS#11	CSP	Java JCE / SunPKCS11	BouncyCastle[24]	Java JCE / CAPI	.NET Crypto
01	Système exploitation	Windows	Y	Y	Y	Y	Y	Y	Y
02		Mac OS X	Y	Y	N/A	Y	Y	Y	N
03		Linux	Y	Y	N/A	Y	Y	Y	Mono ?
04	Langage	C/C++	Y	Y	Y	N/A	N	N/A	Y (C++ managé)
05		Java	Y	Y	Y	Y	Y	Y	N/A

[24] Voir « Annexe – Points d'attention et contournements »

#	Domaine	Section	PC/SC	PKCS#11	CSP	Java JCE / SunPKCS11	BouncyCastle[24]	Java JCE / CAPI	.NET Crypto
06		C#	Y	Y	Y	N/A	Y	N/A	Y
07	**Fonctionnalités**	Accès concurrents[25]	Y	Y	Y	Y	Y	Y	Y
08		Evènements lecteurs	Y	N	N	N	N	N	N
09		Evènements cartes	Y	Y	N	N	N	N	N
10		Optimisation saisie codes porteurs	Y	N	N	N	N	N	N
11		Boite de dialogue de saisie du code porteur	N	N (v5)	Y	N (v5)	N (v5)	Y (CSP)	Y
12		SHA-1	Y	Y	Y	Y	Y	Y	Y
13		SHA-2 (RGS)	Y	Y	N	N	N	N	N
14		Signature	Y	Y	Y	Y	Y	Y	Y
15		Signature « IAS-ECC » (RGS)	Y	Y	Y	N	N	N	N
16		Authentification	Y	Y	Y	Y	Y	Y	Y

[25] Dans le cas où le logiciel GALSS et le protocole PSS sont utilisés, utiliser le GALSS version 3.40.01 ou supérieure.

#	Domaine	Section	PC/SC	PKCS#11	CSP	Java JCE / SunPKCS11	BouncyCastle[24]	Java JCE / CAPI	.NET Crypto
17		Sans contact « Accès certificat Tech. »	Y	Y	Y	Y	Y	Y	Y
18		Sans contact « Accès conteneur de données »	Y	Y	N	N	N	N	N
19		Accès aux objets métiers Santé&Sociale	Y	Y	N	N	N	N	N
20		« Interopérabilité »	Y	Y	N	Y	Y	Y	N
21		« Configurabilité »	Y	Y	N	N	N	N	N
22		Performance	Y	Y	Y	Y	Y	Y	Y
23	**Architecture**	Client lourd	Y	Y	Y	Y	Y	Y	Y
24		Client léger	Y	Y	Y	Y	Y	Y	Y
25		Embarqué	Y	Y	N	N	N	N	N
26	**Expertises**	Expertise carte à puce	Y	N	N	N	N	N	N
27		Expertise Crypto	Y	Y	Y	N	Y	N	N
28		Expertise PKI	Y	Y	Y	N	Y	N	N
29		Expertise programmation	Y	Y	Y	N	Y	N	N

Tableau 138 : Cryptolib CPS: Matrice d'intégration



19.8 Points d'attention et bonnes pratiques

Les portions de code fournies ci-dessus ne peuvent bien évidemment pas partir en production telles quelles. Elles ont le mérite de fonctionner mais elles n'intègrent pas (en particulier) de code assurant:

1. la gestion de la récupération de valeurs de paramètres de configuration
   a. Par exemple : Les valeurs « 1 » (type de CSP) et « ASIP Sante Cryptographic Provider » (nom du CSP) peuvent changer par exemple
2. la gestion des erreurs
3. la génération de log
4. la gestion de présence de plusieurs cartes sur un même poste
5. la recherche de performances spécifiques
   a. cf. « Performances et sécurité »
6. les optimisations
   a. ex. : caches, factories…
   b. ex. : optimisation ergonomiques (saisie de code porteur en dehors du CSP : CryptoKeySecurity et SecureString en .NET)

Par ailleurs, la carte à puce et le lecteur de carte sont deux ressources matérielles qui peuvent en particulier:

1. Tomber en panne
2. Etre arrachés avant ou pendant les opérations fonctionnelles
3. Etre rebranchés sur de nouveaux emplacements
4. Etre lents
5. Etre utilisés par plusieurs applications en parallèle

Au moment d'intégrer la carte CPx, il convient donc :

1. de bien avoir ces contraintes à l'esprit
2. de se plier aux bonnes pratiques énumérées ci-après.

#	Points d'attention et bonnes pratiques
1	Gestion de la récupération de valeurs de paramètres de configuration
2	Gestion des événements matériels
3	Gestion des erreurs
4	Génération des logs
5	Gestion des accès concurrents
6	Gestion de présence de plusieurs cartes sur un même poste
7	Saisie des codes porteurs (code porteur et code de déblocage)
8	Gestion des filières d'accès vers la carte CPx (1 seule filière recommandée, i.e. rationalisation des filières d'accès)

Tableau 139 : Points d'attention et bonnes pratiques

Cryptolib CPS	L'intégration logicielle de la carte CPx est assujettie aux mêmes règles et bonnes pratiques de génie logiciel que tout développement logiciel « classique ».

Tableau 140 : Cryptolib CPS: Remarques bonnes pratiques pour intégration de la carte CPx

19.9 Intégration dans les architectures existantes

19.9.1 Smartcard logon

La carte CPS3 et la Cryptolib CPS v5 sont compatibles avec les mécanismes de Smartcard logon Windows. Leur intégration dans ce type d'architecture fait l'objet d'un guide dédié.

19.9.2 Profils itinérants

La carte CPS3, la Cryptolib CPS v5 et le GALSS sont compatibles avec les fonctionnalités de profils itinérants offerts par les systèmes d'exploitation Microsoft. Leur intégration dans ce type d'architecture fait l'objet d'un guide dédié.

19.9.3 Client léger, TSE et Citrix

La carte CPS3, la Cryptolib CPS v5 sont compatibles avec les architectures client légers implémentés via TSE / Citrix. Leur intégration dans ce type d'architecture est reportée en annexe de ce guide.

Cryptolib CPS	La Cryptolib CPS a pour ambition de respecter au mieux les standards du marché et les architectures des systèmes sur lesquels elle est déployée. La Cryptolib CPS peut dès lors potentiellement être intégrée dans toutes les fonctionnalités de sécurité ou de sécurisation des systèmes d'exploitation qu'elle cible.

Tableau 141 : Cryptolib CPS: Remarques scénarios d'intégration fonctionnelle Cryptolib CPS

20Annexe – Précisions techniques

T	v3	v4	v5	Remarques
1	x	x		En environnement 64 bits, les Cryptolib CPS v3 et v4 fonctionnent en mode émulation 32 bits.
2	x	x		Avec les Cryptolib CPS v3 et v4, les applications utilisées ne peuvent donc être que des applications 32 bits (navigateurs, clients de messagerie, …).
3	x	x		Avec les Cryptolib CPS v3 et v4, le mécanisme de « Smartcard logon » - mis en œuvre de manière native par le système - ne fonctionne pas sur un système 64 bits du fait de l'émulation 32 bits. La Cryptolib CPS v5 64 bits est requise dans ce cas de figure.
4			x	La Cryptolib CPS v5 est compilée pour les systèmes 32 bits ou 64 bits. 2 installeurs MSI différents (1 pour chaque architecture) sont disponibles.
5			x	La Cryptolib CPS v5 32 bits s'installe sur les systèmes 64 bits. Cette configuration est néanmoins fortement déconseillée.
6			x	Avec la Cryptolib CPS v5, les applications 64 bits fonctionnent désormais du fait de la disponibilité de la version 64 bits (IE10+ en mode 64 bits par exemple).
7			x	Avec la Cryptolib CPS v5, le mécanisme de « Smartcard logon » - mis en œuvre de manière native par le système - fonctionne sur un système 64 bits du fait de la disponibilité de la version 64 bits.
8	x			Lors de l'installation de la version GALSS de la Cryptolib CPS v3, le serveur doit disposer préalablement d'au moins un lecteur de carte (PC/SC ou PSS) présent et correctement installé sur le poste.
9	x			Si le serveur tourne dans un environnement virtualisé (type VMware, Hyper-V, XenServer, …), le lecteur de cartes devra être présent sur le poste client pilotant le serveur (pas sur la machine où est hébergé physiquement le serveur). L'utilisateur doit disposer des droits administrateur.
10		x	x	Cette limitation n'a plus cours avec la Cryptolib CPS v4 ou la Cryptolib CPS v5.
11	x	x	x	Excepté dans le cadre du Smartcard logon, l'installation de la Cryptolib CPS se fait exclusivement sur le serveur : aucun composant CPS n'a besoin d'être installé sur les postes client.

Tableau 142 : Précisions techniques

21Annexe – L'IGC de Santé

21.1 Le Certificat X.509

Un certificat X.509 est un message (binaire) électronique écrit suivant une syntaxe définie par la norme X.509 et signé par une autorité pour en garantir l'intégrité et la véracité de ses informations.

Les informations principales certifiées portent sur :

- L'identification de l'autorité ou émetteur, qui a signé ce certificat.
- Les dates de début et de fin de validité du certificat.
- L'identification du sujet ou objet, pour qui a été délivré ce certificat.
- La clé publique RSA[26].

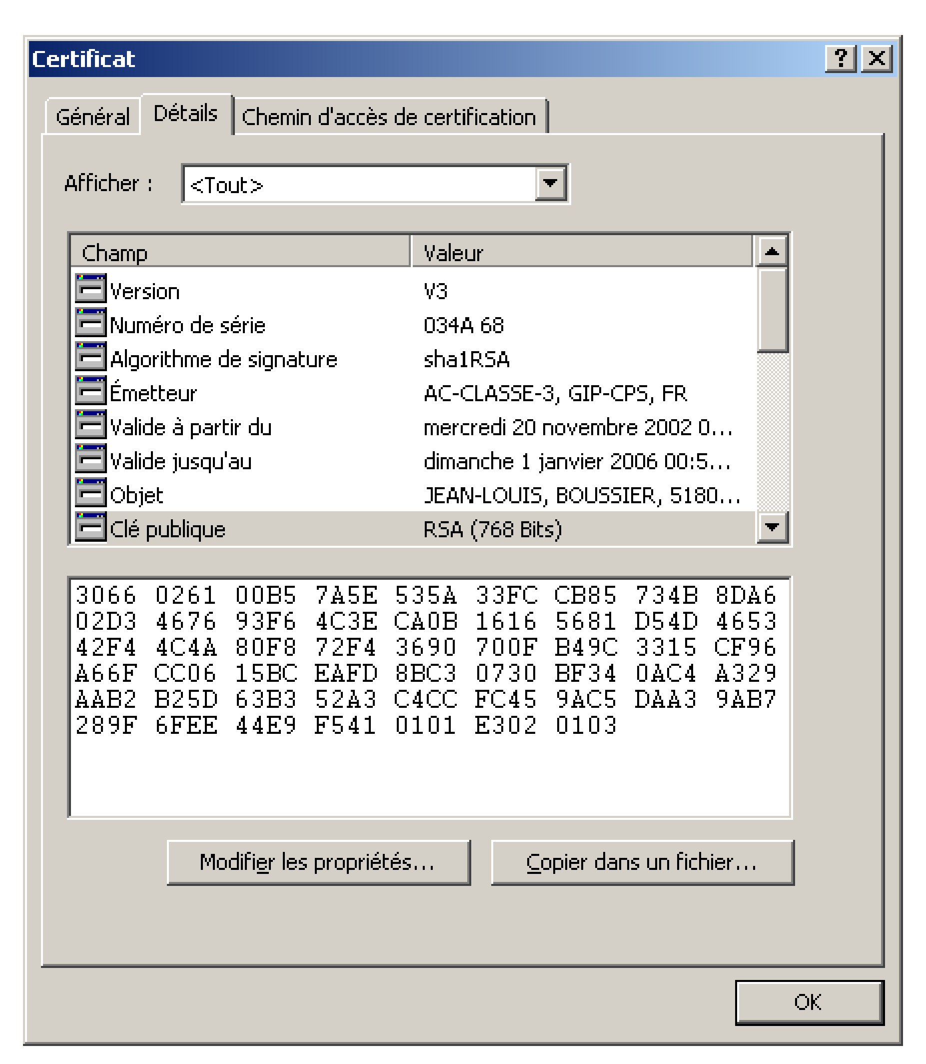


Figure 106 : Exemple d'un certificat X.509 d'authentification d'une CPS2bis (CPA)

[26] L'algorithme cryptographique RSA utilise une clé en deux parties (bi-clé) : l'une est publique (diffusée dans le certificat X.509) et l'autre est privée (gardée secrète dans un coffre-fort logiciel ou dans une carte comme la CPx).

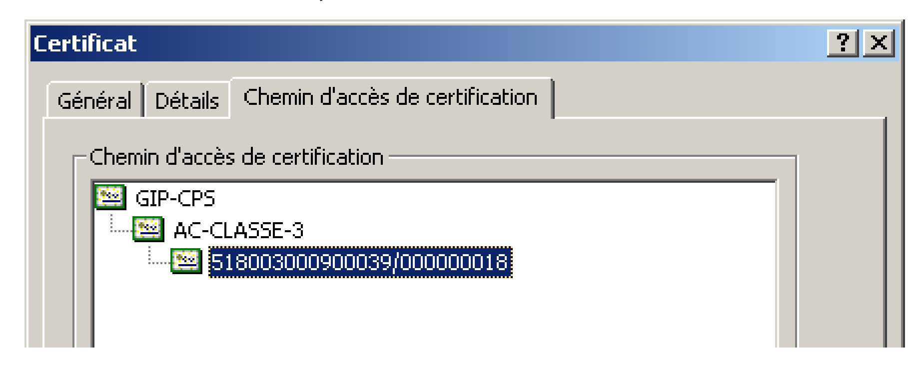
Il existe deux certificats X.509 (donc deux bi-clés) dans une CPx: l'un d'authentification et l'autre de signature, auquel s'ajoute un certificat X.509 « technique » pour la partie sans-contact de la CPS3.

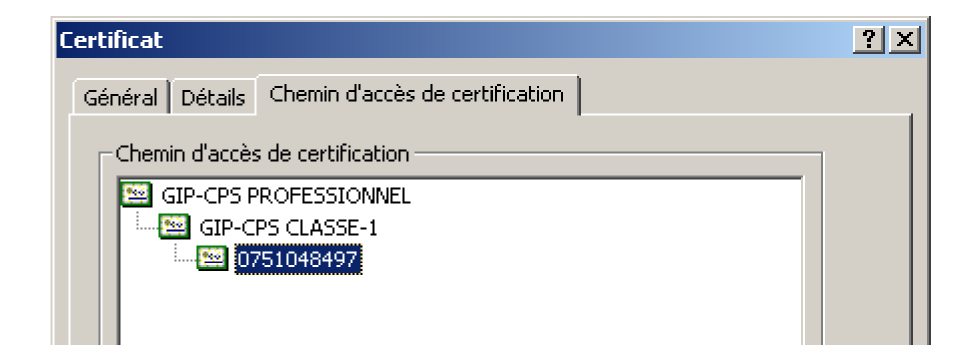
21.2 Chaînes de confiance des certificats X.509 de la carte CPS

Si un certificat X.509 est signé par une autorité de certification. Celle-ci a elle-même un certificat, lui aussi signé par une autorité, et ainsi de suite jusqu'à rencontrer en tête de chaîne un certificat auto-signé (dit Racine ou Root) pour lequel ce sera bel et bien à l'utilisateur de manifester explicitement sa confiance.

Dans le cas de la carte CPS, les certificats racines sont publiés sur le site http://annuaire.asipsante.fr/.

Toutes ces informations peuvent être vérifiées avant d'accorder sa confiance à ces certificats.





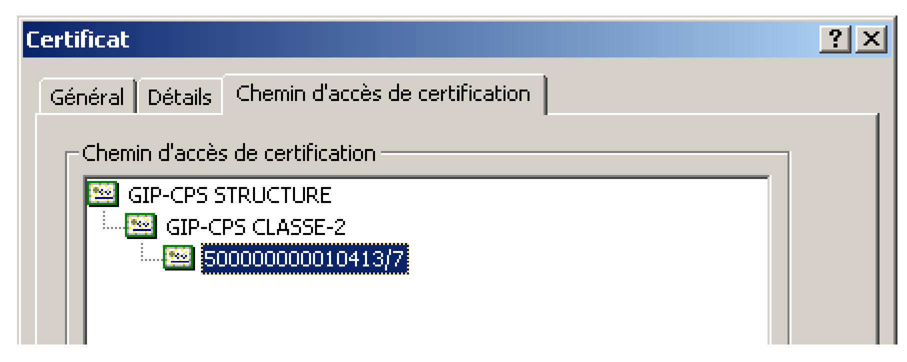


Figure 107 : Exemples de chaînes de confiance de CPS

Figure 108 : d'une CPS2bis (CPA)

Figure 109 : d'une CPS2ter (CPS et CPF)

Figure 110 : d'une CPS2ter (CDE)

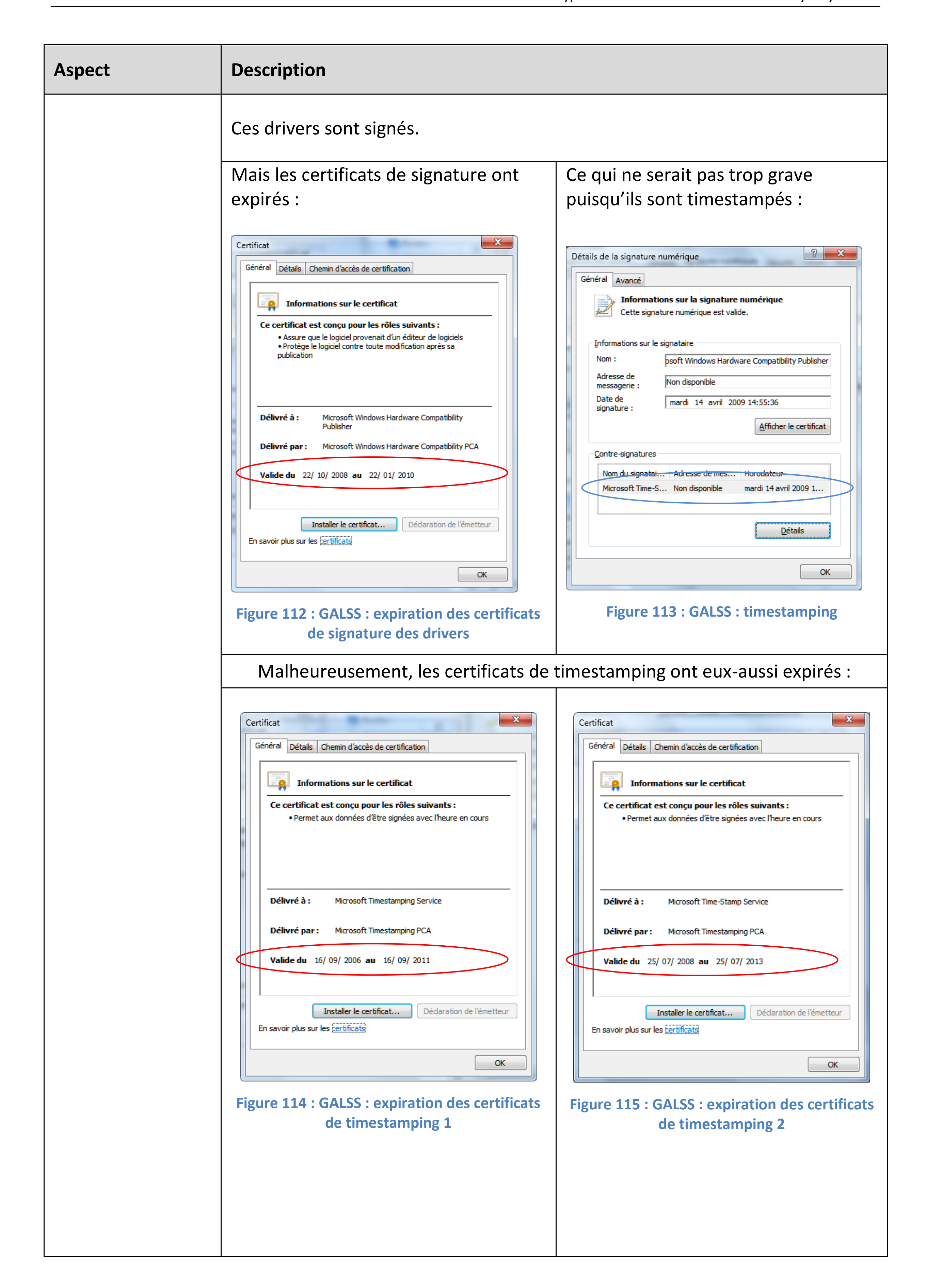
Les données contenues dans les certificats ASIP Santé (« gabarits ») sont exhaustivement décrites dans **[26]**.

22Annexe – Installation du lecteur Xiring Prium 3S – Ingenico IHC800



Figure 111 : lecteur Xiring Prium 3S – Ingenico IHC800

Aspect	Description
Présentation	http://healthcare-eid.ingenico.com/solution_guichet.aspx http://healthcare-eid.ingenico.com/Sante-Terminaux-fixes.aspx
Brochure	http://healthcare-eid.ingenico.com/iso_album/inghe-id_fiche_ihc800_vfr.pdf http://healthcare-eid.ingenico.com/iso_album/inghe-id_fiche_prium-3s_vfr.pdf
Driver USB	http://www.distrimed.com/telechargement/SESAM_VITALE/Pilotes%20Ingenico-Xiring.zip Les drivers sont aussi fournis par le GALSS (répertoire C:\INSTALLS\GALSS\32b\Extract\CommonAppData\santesocial\galss\inf\Lecteur1\, voir « Gestion avancée des drivers lecteur GIE SESAM-Vitale »). Ces drivers sont : xcomusbvista32.cat XComUsbVista32.inf xcomusbvista64.cat XComUsbVista64.inf xcomusbxp32.cat XComUsbXp32.inf xcomusbxp64.cat XComUsbXp64.inf



Aspect	Description	
	Ces drivers sont signés.	
	Mais les certificats de signature ont expirés : Figure 112 : GALSS : expiration des certificats de signature des drivers	Ce qui ne serait pas trop grave puisqu'ils sont timestampés : Figure 113 : GALSS : timestamping
	Malheureusement, les certificats de timestamping ont eux-aussi expirés :	
	Figure 114 : GALSS : expiration des certificats de timestamping 1	Figure 115 : GALSS : expiration des certificats de timestamping 2

Aspect	Description
Windows 8	http://www.distrimed.com/telechargement/NOTICE_WINDOWS8_PILOTE_LECTEUR.pdf
Windows 8.1	http://www.distrimed.com/telechargement/NOTICE_WINDOWS8.1_PILOTE_LECTEUR.pdf
Paramétrage du lecteur	http://www.distrimed.com/telechargement/SESAM_VITALE/PRIUM3S_GUIDE_UTILISATION.pdf
Firmware 3.07	http://www.distrimed.com/telechargement/SESAM_VITALE/PRIUM3S_FIRMWARE_3.07.zip

Tableau 143 : Installation du lecteur Xiring Prium 3S – Ingenico IHC800

23Annexe – Installation et utilisation en environnements TSE / Citrix

23.1 Description de l'installation « GALSS »

23.1.1 Architecture

L'installation décrite ci-après vise à installer les éléments logiciels suivants (vue depuis « écran » client) :

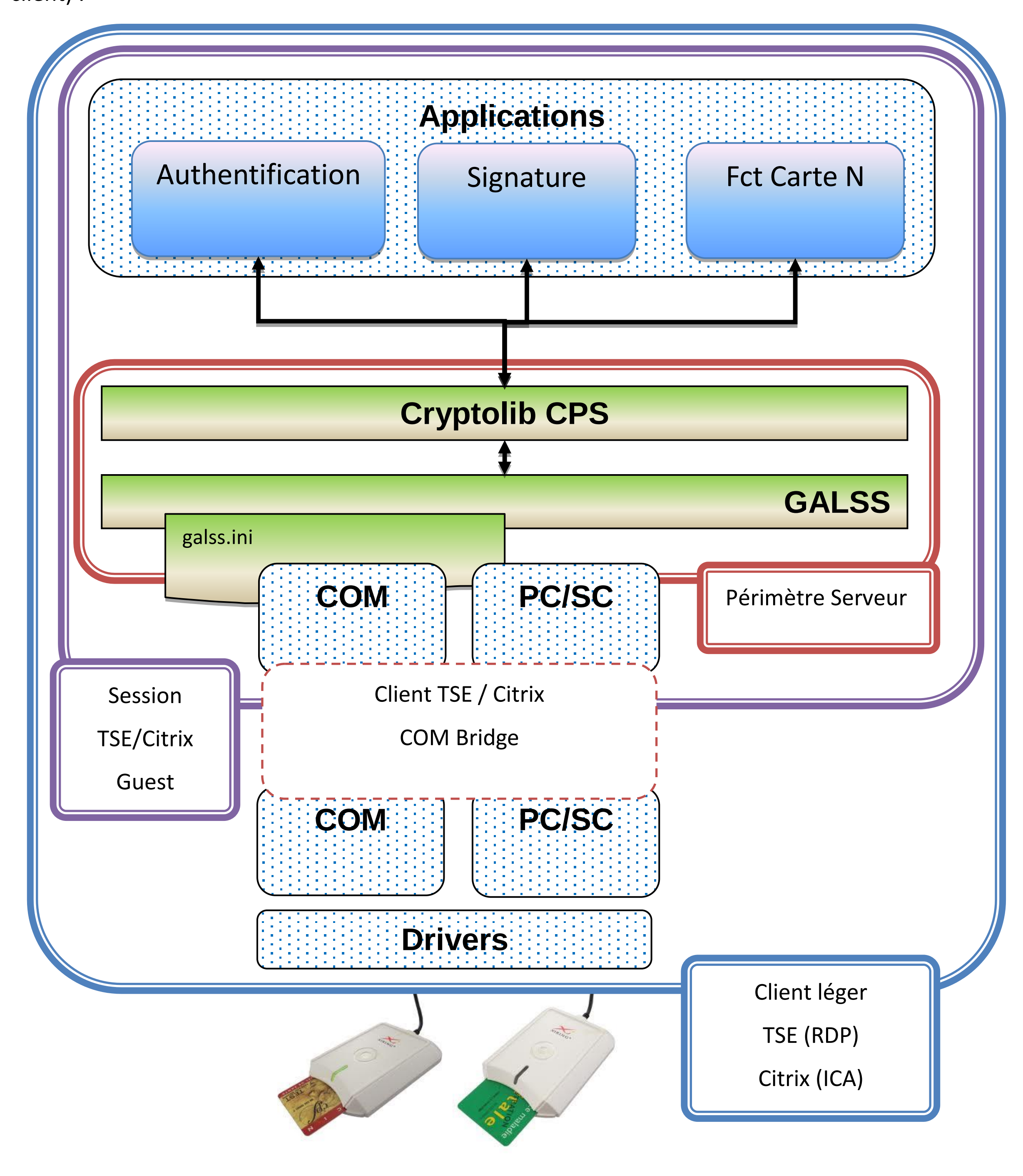


Figure 116 : Architecture Cryptolib CPS TSE/Citrix en filière GALSS

23.1.2 Déroulement

Les droits « administrateur » (tous les droits d'écriture et d'accès) sont requis avant de démarrer la procédure.

#	v3	v4	v5	Description
1	x			Passage en mode « installation » du serveur :
				En ligne de commandes, lancer la commande : **change user /install** (Voir « Annexe »).
		x	x	Cette étape n'est pas requise avec des installeurs MSI http://technet.microsoft.com/en-us/library/cc754288%28WS.10%29.aspx
2	x			Lancer le setup d'installation (.exe) de la Cryptolib CPS sur GALSS pour Windows.
		x	x	Lancer le MSI d'installation (.msi) de la Cryptolib CPS sur GALSS pour Windows.
	x	x	x	Suivre ensuite le déroulement de l'installation comme indiqué dans le manuel d'installation standard de la Cryptolib CPS GALSS.
	x			A la fin de l'installation, le setup demandera de redémarrer votre serveur (pour la version GALSS de la Cryptolib CPS).
		x	x	Ce reboot n'est généralement plus demandé par les installeurs MSI des Cryptolib CPS v4 et v5.
3	x			Passage en mode « exécution » du serveur : en ligne de commandes, lancer la commande : **change user /execute**
				Pour vérifier en quel mode le serveur se trouve, lancer la commande **change user /query**
				Cette étape n'est pas requise avec des installeurs MSI http://technet.microsoft.com/en-us/library/cc754288%28WS.10%29.aspx
4	x	x	x	**Déplacer les 2 fichiers .INI de la Cryptolib CPS (galss.ini et cps_pkcs11_safe.ini) du répertoire %WINDIR% (« C:\Windows » par défaut) vers le sous-répertoire \Windows du répertoire de base de chaque utilisateur %USERPROFILE%\Windows** : 1. par défaut sous W2003 a. « C:\documents and settings\«utilisateur»\Windows\ » 2. par défaut sous W2008 a. « C:\Users\«utilisateur»\Windows\ »
	x	x	x	**Important : Bien vérifier que ces deux fichiers ne sont plus présents dans le répertoire Windows (%WINDIR%, « C:\Windows » par défaut)**

Tableau 144 : Installation en filière GALSS

Remarque 1	Dans le cas où le setup est exécuté sur le serveur, sans être passé en mode « installation », tous les fichiers seront copiés : • dans le répertoire de base de l'utilisateur %USERPROFILE%\Windows • par défaut sous W2003 : « C:\documents and settings\«utilisateur»\Windows » • par défaut sous W2008 : « C:\Users\«utilisateur»\Windows\ »
	Il faudra alors recopier tous ces fichiers dans le répertoire %WINDIR% (« C:\Windows\ » par défaut), **à l'exception** du galss.ini et cps_pkcs11_safe.ini.
Remarque 2	La logique voudrait que tous les postes client soient correctement installés et configurés. Cela implique que les pilotes de chaque périphérique soient installés correctement (pilotes, port). Cela concerne en particulier les lecteurs bi-fente. 2 cas de figure : 1. le lecteur bi-fente est branché sur un port série 2. le lecteur bi-fente est branché sur un port USB avec une émulation de port série virtuel (driver USB <-> COM) Dans le premier cas, TSE/Citrix fonctionnera avec la redirection de port COM sans qu'il soit nécessaire d'installer les drivers du lecteur sur le serveur. Dans le deuxième cas, TSE/Citrix devrait fonctionner avec la redirection de port COM sans qu'il soit nécessaire d'installer les drivers du lecteur sur le serveur, de la même manière que pour le cas 1. Cependant, la redirection série d'un port COM virtuel peut poser problème dans certains cas (à tester au cas par cas). Dans ce cas, il peut être préférable : • d'installer aussi le driver USB/série sur le serveur • d'effectuer ensuite une redirection du périphérique USB du client vers le serveur

Tableau 145 : Remarques filière GALSS

23.1.3 Vérification du bon fonctionnement de la Cryptolib CPS

#	Vérification
1	Installer et configurer un poste client léger (lecteur de carte connecté, drivers installé, client RDP ou Client ICA installé)
2	Lancer une session distante TSE ou Citrix depuis ce poste léger
3	Lancer l'application CPS-Gestion (« cpgesw32.exe »).
4	Les données de la carte insérée seront affichées à l'écran, si l'installation s'est bien déroulée.

Tableau 146 : Vérification installation en filière GALSS

23.1.4 Paramétrage

<table>
<tr><th>#</th><th>v3</th><th>v4</th><th>v5</th><th colspan="2">Description</th></tr>
<tr><td rowspan="5">1</td><td>x</td><td>x</td><td>x</td><td colspan="2">Chaque utilisateur du service TSE (ou surcouche CITRIX) devra donc avoir dans son répertoire personnel %USERPROFILE%\Windows, un fichier galss.ini.</td></tr>
<tr><td></td><td>x</td><td>x</td><td colspan="2">De ce fait, le fichier de configuration galss.ini n'est pas propre au serveur physique (qui n'a d'ailleurs généralement pas de lecteur) mais au couple {poste physique léger, compte utilisateur}.</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">x</td><td rowspan="2">x</td><td colspan="2">Pour une utilisation des comptes utilisateur de manière nomade et avec des configurations de poste hétérogènes (ayant des configurations de lecteurs différentes), il faudra manuellement importer un fichier galss.ini correspondant à la configuration des lecteurs du poste dans le profil de l'utilisateur.</td></tr>
<tr><td colspan="2">Suivant la configuration des profils itinérants, cette opération sera à réaliser à chaque ouverture de session ou non.</td></tr>
<tr><td></td><td>x</td><td>x</td><td colspan="2">Cette opération peut se faire à l'aide par exemple d'un script d'ouverture de session, qui recopiera le bon galss.ini, en fonction du poste client.</td></tr>
<tr><td rowspan="3">2</td><td>x</td><td>x</td><td>x</td><td colspan="2">Version GALSS : chaque utilisateur TSE/CITRIX, devra avoir les droits en écriture sur le répertoire :
• %ALLUSERSPROFILE%\santesocial\CPS\Coffre\
• C:\Documents and settings\all users\santesocial\CPS\Coffre\ par défaut sous W2003
• C:\ProgramData\santesocial\CPS\Coffre ou C:\Users\All Users\santesocial\CPS\Coffre\ par défaut sous W2008 (attention aux liens symboliques sous cet OS).</td></tr>
<tr><td>x</td><td>x</td><td></td><td colspan="2">Le fichier de cache « ccert.bin » doit pouvoir être modifié à tout moment par la Cryptolib CPS.</td></tr>
<tr><td></td><td></td><td>x</td><td colspan="2">Le fichier de cache « ccert.bin » n'est plus géré par la Cryptolib CPS v5.

En lieu et place, la Cryptolib CPS v5 utilise plusieurs fichiers situés dans : %ALLUSERSPROFILE%\santesocial\CPS\cache\</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">x</td><td rowspan="3">x</td><td rowspan="3">x</td><td colspan="2">Configurer la redirection des lecteurs de carte du poste client vers le serveur, en fonction de leur type :</td></tr>
<tr><td>lecteur PSS série</td><td>cocher l'option port série des options TSE (connexion TSE), et lancer la commande « net use com1 : \\client\com1 » (connexion ICA CITRIX)</td></tr>
<tr><td>lecteur PC/SC</td><td>cocher l'option « lecteur de cartes à puce » dans ressources locales (connexion TSE).</td></tr>
</table>

Tableau 147 : Paramétrage filière GALSS

23.2 Description de l'installation « Full PC/SC »

Pour la version PC/SC, et en environnement Client/serveur, aucune manipulation particulière (présence préalable de lecteur de carte…) n'est nécessaire (pas de GALSS installé).

23.2.1 Architecture

L'installation décrite ci-après vise à installer les éléments logiciels suivants (vue « écran » client) :

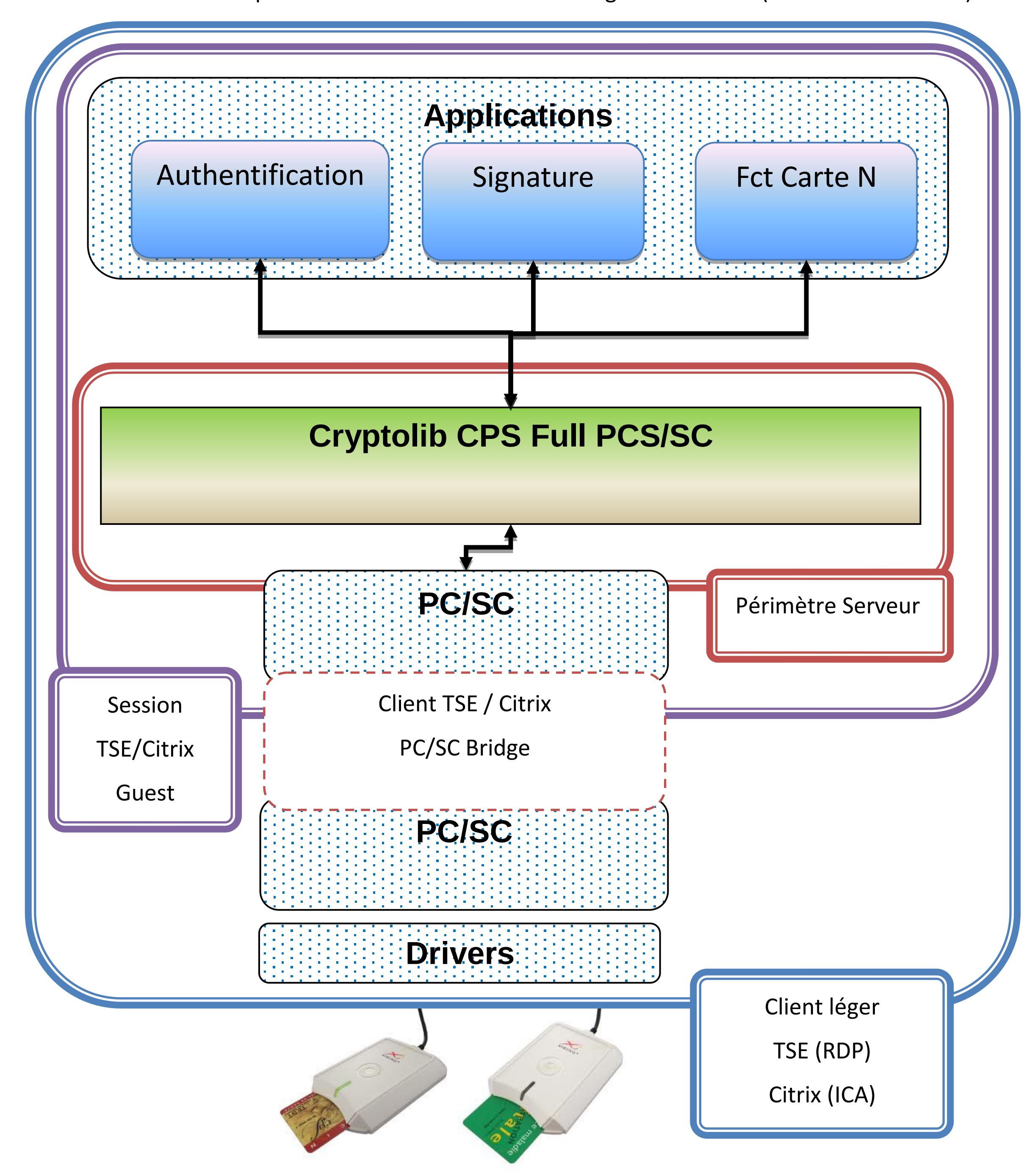


Figure 117 : Architecture Cryptolib CPS TSE/Citrix en filière PC/SC

23.2.2 Déroulement

La procédure doit être démarrée sous un compte administrateur du serveur.

#	v3	v4	v5	
1	x	x	x	Lancer le setup d'installation de la Cryptolib CPS PC/SC pour Windows.
	x	x	x	Suivre ensuite, le déroulement de l'installation comme indiqué dans le manuel d'installation standard de la Cryptolib CPS PC/SC.

Tableau 148 : Installation en filière PC/SC

23.2.3 Vérification du bon fonctionnement de la Cryptolib CPS

#	Vérification
1	Lancer l'application CPS-Gestion (« cpgesw32.exe »).
2	Les données de la carte insérée seront affichées à l'écran, si l'installation s'est bien déroulée.

Tableau 149 : Vérification installation en filière PC/SC

23.2.4 Paramétrage

#	v3	v4	v5	
1	x	x	x	La version PC/SC de la Cryptolib CPS gère en interne automatiquement les différentes configurations de poste (lecteurs de carte).
				Aucune configuration particulière des comptes utilisateur n'est donc nécessaire, y compris lors d'une mise en œuvre des profils itinérants.
2	x	x	x	Lecteur PC/SC : Seule la redirection des lecteurs PC/SC de carte à puce du poste client vers le serveur devra être activée. Cocher l'option « lecteur de cartes à puce » dans ressources locales (connexion TSE).

Tableau 150 : Paramétrage filière PC/SC

23.3 Emplacements des fichiers

Ce Chapitre détaille les emplacements des fichiers de la Cryptolib CPS, dans un environnement Client/serveur.

23.3.1 Chemin d'accès profil utilisateur [USER]

En fonction du système d'exploitation hôte et du paramétrage des comptes utilisateurs, le chemin d'accès au profil utilisateur peut être différent :

Par défaut en local	Windows 2003 : %USERPROFILE% = C:\documents and settings\«utilisateur»\ par défaut
	Windows 2008 : %USERPROFILE% = C:\utilisateurs\«utilisateur»\ ou C:\users\«utilisateur»\ par défaut
Par profil itinérant à distance	Si des profils itinérants ont été définis, ces profils utilisateurs peuvent être stockés sur un partage réseau à distance.
	Deux façons de gérer ces emplacements : 1. depuis l'Active Directory du contrôleur de domaine -> users -> propriété d'un utilisateur -> profil -> chemin du profil 2. à partir de GPO = stratégies de groupes. Voir avec votre administrateur de domaine, pour plus de détails.
	Dans ce cas, la résolution du chemin du profil de l'utilisateur se fait ainsi (Windows 2003 et 2008 Server): [USER] = %HOMEDIR%%HOMEPATH%, ou %HOMEDIR% et %HOMEPATH% sont deux variables d'environnement, définissant le chemin d'accès du profil utilisateur distant. Ces variables sont accessibles avec la commande SET en ligne de commandes DOS. Ces variables ne sont pas définies si les profils itinérants ne sont pas utilisés.

Tableau 151 : Chemins des profils utilisateur

23.4 Lignes de commande

Ce chapitre reprend la documentation de « `change user` » et « `change port` ».

Cette documentation permet de comprendre le fonctionnement de TSE.

23.4.1 Commande « change user »

Modifie le paramétrage relatif au mappage du fichier .ini.

23.4.1.1 Syntaxe

```
change user {/execute | /install | /query}
```

23.4.1.2 Paramètres

`/execute`	Active le mappage du fichier .ini au répertoire de base. Il s'agit du paramètre par défaut.
`/install`	Désactive le mappage du fichier .ini au répertoire de base. Tous les fichiers .ini sont lus et enregistrés dans le répertoire système. Le mappage du fichier .ini doit être désactivé lors de l'installation des applications sur un serveur Terminal Server.
`/query`	Affiche le paramétrage actuel relatif au mappage du fichier .ini.
`/?`	Affiche l'aide à l'invite de commandes.

Tableau 152 : Paramètres de la commande « Change user »

23.4.1.3 Remarques

R	Remarques sur l'utilisation de la commande « Change user »
1	Utilisez la commande **`change user /install`** avant d'installer une application, pour créer des fichiers .ini pour cette application dans le répertoire système.
	Ces fichiers servent de sources pour les fichiers .ini spécifiques aux utilisateurs. Après avoir installé l'application, utilisez la commande **`change user /execute`** pour revenir au mappage du fichier .ini standard.
2	La première fois que l'application est exécutée, elle recherche ses fichiers .ini dans le répertoire de base.
	Si les fichiers .ini ne se trouvent pas dans le répertoire de base mais dans le répertoire système, ces fichiers sont copiés dans le répertoire de base par les services Terminal Server, garantissant ainsi que chaque utilisateur dispose d'une copie unique des fichiers .ini de l'application. Les nouveaux fichiers .ini sont créés dans le répertoire de base.
3	Chaque utilisateur doit disposer d'une copie unique des fichiers .ini d'une application.
	Cela permet d'éviter les situations où différents utilisateurs possèdent des configurations d'applications incompatibles, par exemple, des répertoires par défaut ou des résolutions d'écran qui ne sont pas les mêmes.

R	Remarques sur l'utilisation de la commande « Change user »	
4	Lorsque le système est en mode Installation (`change user /install`), plusieurs événements se produisent :	
	1	Toutes les entrées du Registre créées sont masquées sous HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\TerminalServer\Install
	2	Les clés ajoutées à HKEY_CURRENT_USER sont copiées sous la clé \SOFTWARE, tandis que les clés HKEY_LOCAL_MACHINE sont copiées sous \MACHINE.
	3	Si l'application interroge le répertoire Windows en utilisant des appels système, comme GetWindowsDirectory, les services Terminal Server renvoient le répertoire Racine Système
	4	Si des entrées de fichier .ini sont ajoutées à l'aide d'appels système, comme WritePrivateProfileString, elles sont ajoutées aux fichiers .ini sous le répertoire Racine Système.
5	Lorsque le système revient en mode d'exécution (**`change user /execute`**), et que l'application tente de lire une entrée du Registre sous HKEY_CURRENT_USER qui n'existe pas, les services Terminal Server vérifient si une copie de la clé existe sous la clé \TerminalServer\Install.	
	1	Si c'est le cas, les clés sont copiées à l'emplacement approprié sous HKEY_CURRENT_USER.
	2	Si l'application tente de lire un fichier .ini qui n'existe pas, les services Terminal Server recherchent ce fichier .ini sous la racine système.
	3	Si le fichier .ini se trouve à la racine système, il est copié dans le sous-répertoire \Windows du répertoire de base de l'utilisateur.
	4	Si l'application interroge le répertoire Windows, les services Terminal Server renvoient le sous-répertoire \Windows du répertoire de base de l'utilisateur.
6	Lorsqu'une session est ouverte, les services Terminal Server vérifient si ses fichiers système .ini sont plus récents que les fichiers .ini qui se trouvent sur votre ordinateur.	
	1	Si la version système est la plus récente, votre fichier .ini est soit remplacé soit fusionné avec cette version. Ceci dépend du fait que le bit INISYNC, 0x40, a été défini ou non pour ce fichier .ini. La version précédente de votre fichier .ini est renommée en Inifile.ctx.
	2	Si les valeurs du Registre du système sous la clé \TerminalServer\Install sont plus récentes que la version située sous HKEY_CURRENT_USER, alors votre version des clés est supprimée et remplacée par les nouvelles clés situées sous \TerminalServer\Install.

Tableau 153 : Fonctionnement de la commande « Change user »

23.4.2 Commande « change port » (changer le port)

Répertorie ou modifie les mappages du port COM pour maintenir la compatibilité avec les applications MS-DOS.

23.4.2.1 Syntaxe

```
Change port [{portx=porty|/d portx|/query}]
```

23.4.2.2 Paramètres

`portx=porty`	Mappe le port COM x au port y.
`/d portx`	Supprime le mappage du port COM x.
`/query`	Affiche les mappages de port actuels.
`/?`	Affiche l'aide à l'invite de commandes.

Tableau 154 : Paramètres de la commande « Change port »

23.4.2.3 Remarques

R	**Remarques sur l'utilisation de la commande « Change port »**
1	La plupart des applications MS-DOS ne prennent en charge que les ports séries COM1 à COM4. La commande « `change port` » mappe un port série vers un autre numéro de port, permettant ainsi aux applications qui ne gèrent pas un nombre important de ports COM d'accéder au port série. Par exemple, pour mapper le port COM12 au port COM1, afin de le rendre utilisable par une application MS-DOS, il suffit d'entrer la commande « `change port com12=com1` ». La modification de mappage ne fonctionne que pour la session en cours. Cette modification n'est pas conservée lorsqu'une session est fermée puis rouverte.
2	Utilisez la commande change port sans paramètres pour afficher les ports COM disponibles et leurs mappages actuels.

Tableau 155 : Fonctionnement de la commande « Change port »

23.4.3 Configuration du fichier galss.ini

23.4.3.1 Configuration du fichier galss.ini en mode serveur

En environnement serveur (Windows 2003, 2008), l'installateur du GALSS ne configure pas le fichier **galss.ini** avec les lecteurs présent sur le serveur.

Dans ce cas de figure, un fichier galss.ini par défaut est installé et ne correspond pas à la configuration matérielle.

Une fois l'installation terminée, il faut donc configurer manuellement le fichier **galss.ini**, sur le serveur ainsi que sur les postes client si besoin :

- Le manuel utilisateur du GALSS (**galss-mu-005_galss3.xx_V1.6.pdf**)
- L'utilitaire « **inigalss.exe** » aidant à la configuration du galss.ini, fourni par le GIE SESAM-Vitale en dehors de l'installeur GALSS

Cf. exemples de fichiers galss.ini en annexe.

23.4.4 Installer des applications sur Terminal Server

3 méthodes (exclusives) au choix :

ID	Méthode
1	Using the Install Application on Terminal Server tool in Control Panel\Programs. This tool is available only when we install terminal server in App mode. It will automatically put terminal server into execute mode when application installation is complete.
2	Run `Change user /install` from command prompt to place the server into Install mode and **install the application**. After installing the application, use the `Change user /execute` command (or restart the server) to place the server back into Execute mode before using the application.
3	**Double click on the MSI**. On a terminal server in App mode, it automatically installs it in Install Mode.

Tableau 156 : Installation des applications sur Terminal Server : Méthodes

Méthode 1: To put Terminal server in application mode
Control Panel -> Add/Remove programs -> Add Windows component -> Terminal Services. If you are running Windows 2000, you will be given an additional choice between Remote Administration and Application Server mode. If you are running Windows 2003, you will not be given this choice, since installing Terminal Services on Windows 2003 already implies Application Server mode.

Tableau 157 : Installation des applications sur Terminal Server : Méthode 1

Méthode 2: Références
How to install application on Windows 2008 Terminal Server
TS RemoteApp Step-by-Step Guide
Remote Desktop Services in Windows 2008 R2 – Part 1 – Installation (with screenshots)
Remote Desktop Services in Windows 2008 R2 – Part 2 – RD Gateway (with screenshots)
Remote Desktop Services in Windows 2008 R2 – Part 3 – RD Web Access & RemoteApp (with screenshots)
Terminal Server Installation

Tableau 158 : Installation des applications sur Terminal Server : Méthode 2

Méthode 3: Cas MSI
Terminal Server Installation: "If you install a program from an .msi package, you do not have to run these commands to switch the system in and out of install mode. Instead, you can run the .msi package or associated Setup file directly."

Tableau 159 : Installation des applications sur Terminal Server : Méthode 3

23.4.5 Prérequis des environnements TSE/CITRIX

Pour que la librairie Cryptolib CPS PC/SC fonctionne correctement en environnement TSE/CITRIX,

Il faut donner un droit particulier (privilège) aux comptes utilisateurs de la librairie:

« Créer des objets globaux ». (SeCreateGlobalPrivilege)

(Que les utilisateurs standards n'ont pas par défaut en environnement TSE/CITRIX)

Manipulation :

1 - Console MMC -> « stratégies ordinateur local » -> « configuration ordinateur » ->

« Paramètres Windows » -> « paramètres de sécurité » -> « stratégies locales » -> « attribution des droits utilisateur » -> « créer des objets globaux »

2 - Ajoutez les comptes utilisateurs concernés.

Plus de détails ici :

http://msdn.microsoft.com/en-us/library/bb530716%28v=VS.85%29.aspx

23.4.6 Configuration des redirections des interfaces lecteurs

Configurer la redirection des lecteurs de carte du poste client vers le serveur, en fonction de leur type :

- lecteur PSS série (lecteur dit « bi-fente ») : cocher l'option port série des options TSE (connexion TSE), et lancer la commande « `net use com1 : \\client\com1` » (connexion ICA CITRIX)
- lecteur PC/SC : cocher l'option « lecteur de cartes à puce » dans ressources locales (connexion TSE).

23.4.7 Réplication des configurations, configurations dynamiques

Dans une architecture client/serveur en production, il est courant d'avoir plusieurs serveurs TSE/CITRIX fonctionnant en parallèle (fermes de serveurs, redondance, etc…).

La procédure d'installation décrite dans ce document concernant la partie serveur (installation et configuration) doit donc être appliquée à chaque serveur de l'architecture concernée afin d'avoir des serveurs configurés de la même manière:

- Installation dupliquée sur chaque serveur
- Configuration dynamique du fichier galss.ini ainsi que de tout autre fichier de configuration lié à l'utilisateur et/ou au poste client à appliquer sur chaque serveur (sauf si les répertoires utilisateurs sont centralisés en un seul emplacement (=profils itinérants))

24Annexe – Exemples de fichier galss.ini

24.1 Exemple de fichier galss.ini pour un poste utilisant un lecteur bi-fente

```
;Fichier de configuration du GALSS dans l'environnement Windows

[PROTOCOLE0]
Config=1000,20,15000
NomLib=PSSINW32.DLL

[CONFIG]
NbCanaux=1

[CANAL1]
TCanal=1
Index=1
Protocole=0
Caracteristiques=9600,1,8,0,0
NbPAD=1

[CANAL1.PAD1]
PAD=2
NbLAD=3

[CANAL1.PAD1.LAD1]
LAD=1
NomLAD=CPS
NbAlias=1
NomAlias1=TRANSPA1

[CANAL1.PAD1.LAD2]
LAD=0
NomLAD=Log_SV
NbAlias=0

[CANAL1.PAD1.LAD3]
LAD=2
NomLAD=Vitale
NbAlias=1
NomAlias1=TRANSPA2
```

Tableau 160 : Exemple de fichier GALSS.INI pour un poste utilisant un lecteur bi-fente

24.2 Exemple de fichier galss.ini pour un poste utilisant deux lecteurs PC/SC

```
;Fichier de configuration du GALSS dans l'environnement Windows.
;Protocole PC/SC

[PROTOCOLE1]
Config=0
NomLib=PCSCW32.DLL
ListeCanaux=1,2

[CONFIG]
NbCanaux=2

[CANAL1]
TCanal=3
Index=1
Protocole=1
Caracteristiques=OMNIKEY CardMan 3x21 0
NbPAD=1

[CANAL1.PAD1]
PAD=0
NbLAD=1

[CANAL1.PAD1.LAD1]
LAD=1
NomLAD=CPS
NbAlias=1
NomAlias1=TRANSPA1

[CANAL2]
TCanal=3
Index=2
Protocole=1
Caracteristiques=OMNIKEY CardMan 3x21 1
NbPAD=1

[CANAL2.PAD1]
PAD=0
NbLAD=1

[CANAL2.PAD1.LAD1]
LAD=1
NomLAD=Vitale
NbAlias=1
NomAlias1=TRANSPA2
```

Tableau 161 : Exemple de fichier GALSS.INI pour un poste utilisant deux lecteurs PC/SC

25Annexe – Windows 7 et icônes de barre de tâche

#	Point d'attention
1	Sous Windows 7, le « Gestionnaire de certificat CPS » (CCM) est masqué, ce qui empêche l'utilisateur de voir l'état de sa carte dans le lecteur

#	Solution
1	Configuration du système suivant la procédure suivante

1er paramétrage: configurer la zone de notification pour que tous les icônes soient toujours visibles :

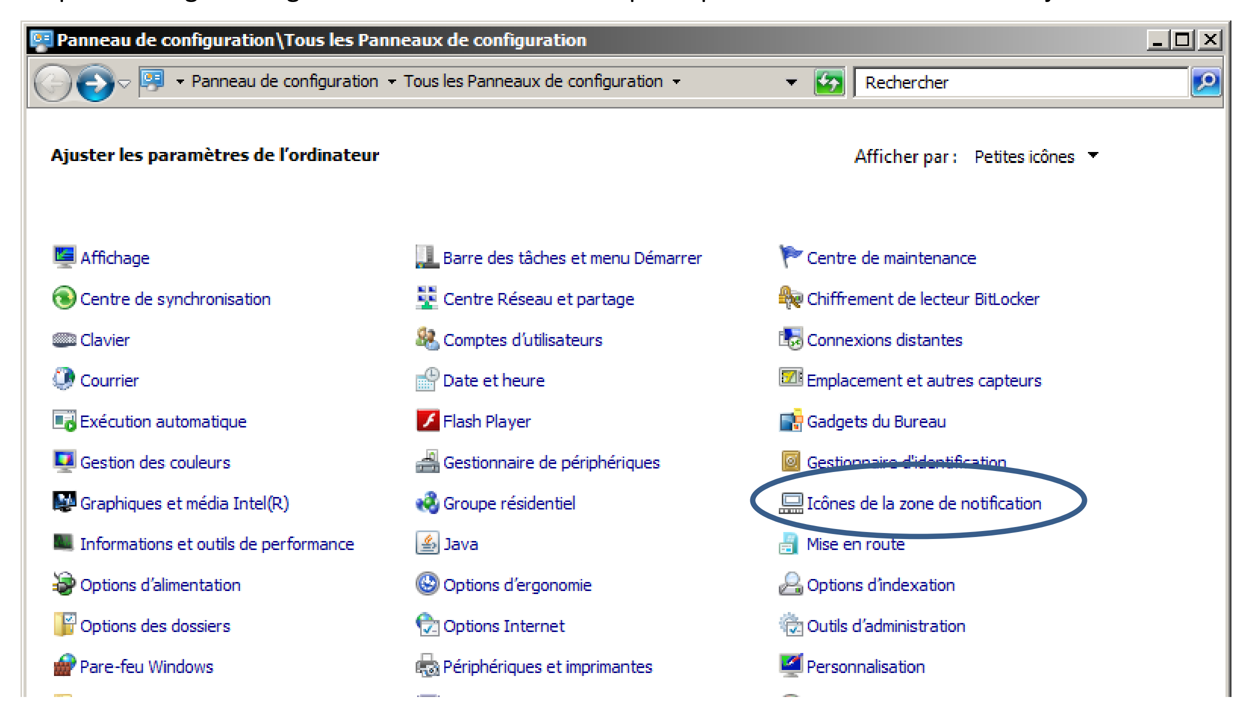


Figure 118 : Windows : Configuration : Paramétrage des icônes de la zone de configuration depuis le panneau de configuration



Figure 119 : Windows : Configuration : Paramétrage des icônes de la zone de configuration depuis la barre de tâches

La fenêtre suivante apparaît.

Cocher l'option « **Toujours afficher toutes les icônes et les notifications sur la barre des tâches** » :

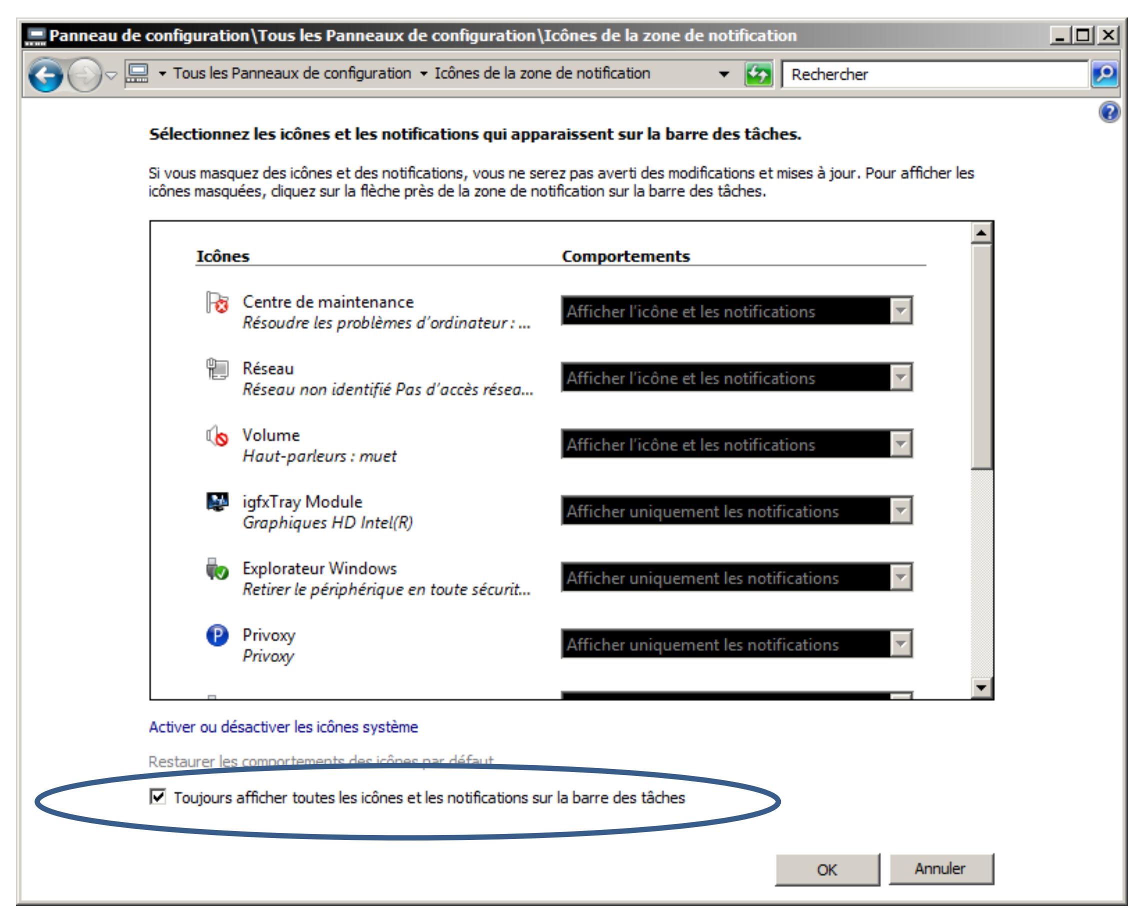


Figure 120 : Windows : Configuration : Afficher tous les icônes

Ceci permet d'avoir tout le temps sous les yeux l'état du lecteur de carte et de la carte dans le lecteur de carte :



Figure 121 : Windows : Configuration : Tous les icônes toujours visibles dans la barre de tâches

Cette opération peut se faire par édition de la base de registre :

Clé	**[HKEY_CURRENT_USER\SOFTWARE \Microsoft\Windows\CurrentVersion\Explorer]** **[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]**		
0001	**Valeur**	**Type**	**Valeurs possibles**
	EnableAutoTray	REG_DWORD	0 = display inactive icons 1 = hide inactive icons

Tableau 162 : Windows : Configuration : Rendre tous les icônes toujours visibles via la base de registre

Autre possibilité : configurer le Gestionnaire de certificat CPS pour qu'il soit toujours visible:

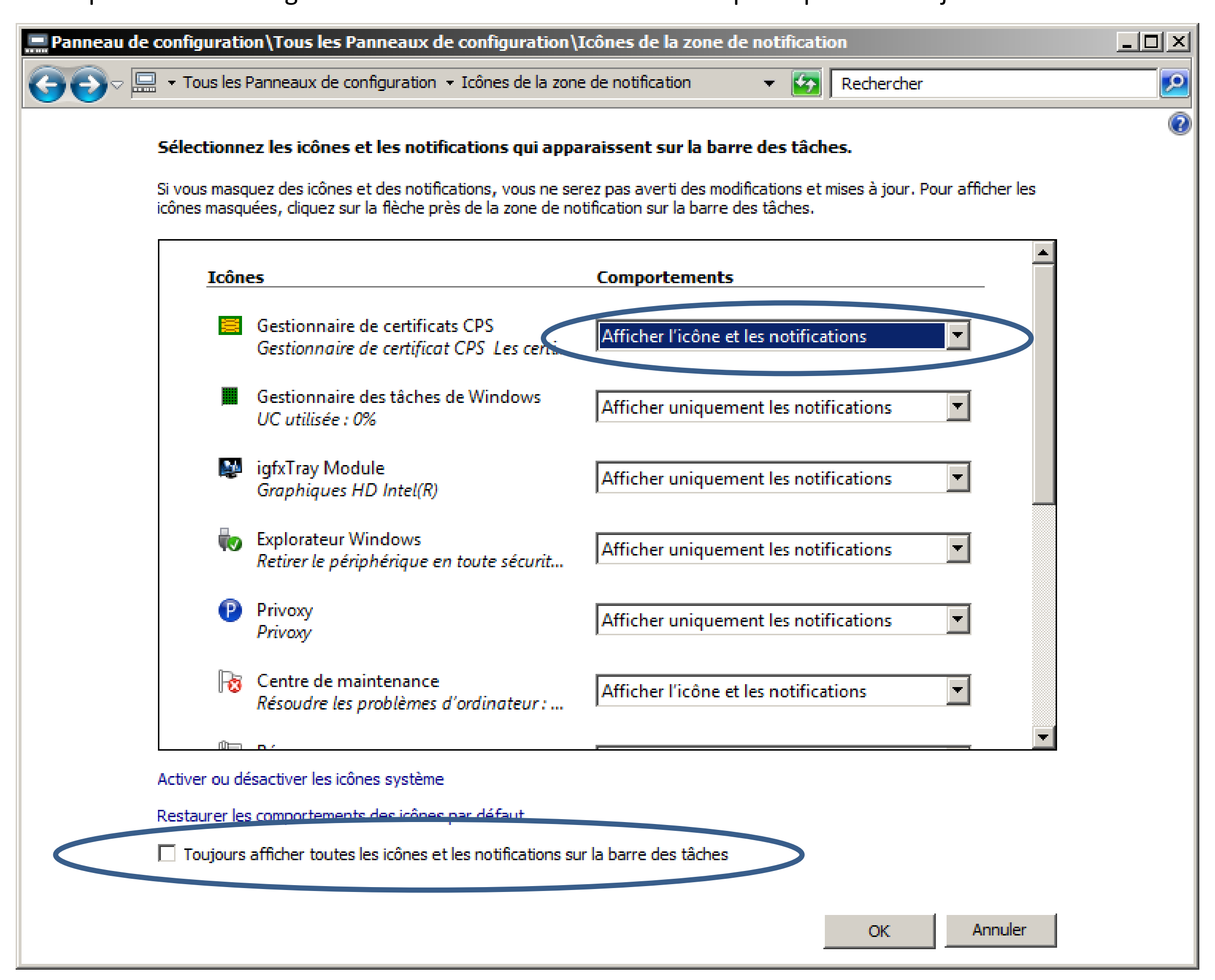


Figure 122 : Windows : Configuration : Gestionnaire de certificat CPS toujours visible

Dans ce cas de figure, l'option « **Toujours afficher toutes les icônes et les notifications sur la barre des tâches** » reste décocher et la configuration se fait spécifiquement pour l'icône du Gestionnaire de certificats CPS en choisissant le comportement « **Afficher l'icône et les notifications** ».

26Annexe – Virtualstore et UAC

Le « **Virtualstore** » est un mécanisme de « **Sandbox** » complémentaire à **l'UAC** présent depuis Windows Vista pour gérer les applications « non compatible UAC ». Il permet d'enregistrer les modifications apportées aux objets « virtualisés » dans le profil de l'utilisateur courant et non pour tous les utilisateurs de l'ordinateur. Il permet ainsi de résoudre des problèmes de compatibilité lorsque l'UAC est activé.

Ce mécanisme de sandbox n'est pas actif si l'UAC est désactivé.

Ce mécanisme n'est pas systématiquement mis en œuvre (http://msdn.microsoft.com/en-us/library/bb530410.aspx).

En particulier, celui-ci est désactivé pour les applications 64 bits ou les applications spécifiant explicitement le comportement à adopter par l'UAC lors d'une demande d'élévation de privilège (fichier manifest contenant l'attribut requestedExecutionLevel).

Le Gestionnaire des Accès aux Lecteurs Santé Social (GALSS) fonctionne en mode client/server. Les API (CPS/ PKCS11 …) sont les clients du processus GALSVW32 qui gère l'accès aux lecteurs physiques. Deux processus vont donc toujours entrer en jeu :

1. le processus server (GALSVW32)
2. le processus client qui charge l'API

Le gestionnaire de tâches Windows permet de vérifier si la virtualisation est activée (colonne virtualisation)

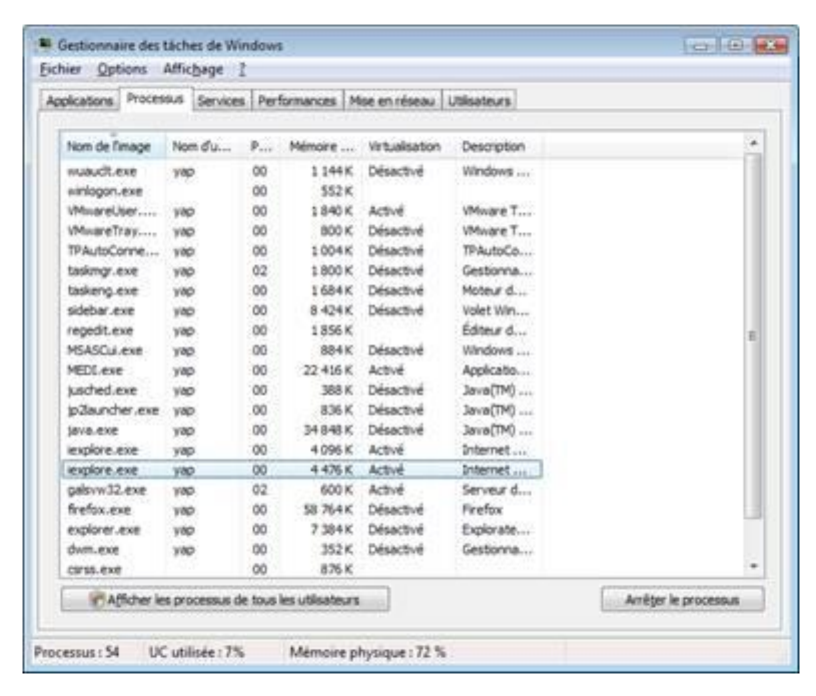


Figure 123 : Vérification de la virtualisation avec le gestionnaire de tâches Windows

La virtualisation est activée pour GALSVW32 / CPS-Gestion / CCM utilisent le galss.ini

La virtualisation est désactivée pour Java / Firefox.

La virtualisation est activée pour Internet Explorer mais Internet Explorer tourne en mode Low Integrity Level (il n'utilise donc pas le virtualstore de l'utilisateur)

L'utilitaire **mt.exe** permet d'étudier les fichiers manifests des différentes applications.

Application	Fichier manifest
GALSVW32	ne contiennent pas de fichier manifest
CPS-Gestion	
CCM	
Internet Explorer	contiennent un fichier manifest avec l'attribut requestedExecutionLevel
Java	
Firefox	
LPS	ne contiennent généralement pas de fichier manifest ou d'attribut requestedExecutionLevel

Tableau 163 : Bilan fichier manifest / attribut requestedExecutionLevel

Le comportement observé est alors conforme aux spécifications de l'UAC : seuls les applications « non compatible UAC » utilisent le virtualstore.

Aucune application Windows native fournie par l'ASIP Santé ou le GIE SESAM-Vitale n'est actuellement réellement compatible avec l'UAC.



27Annexe – Guidelines logiciels Poste de travail

#	Guideline
1	Le mécanisme de virtualisation doit être utilisé au minimum, Microsoft prévoyant de supprimer ce mécanisme dans les prochaines versions de Windows. Ce mécanisme est déjà désactivé pour les applications 64 bits.
2	Le mécanisme de virtualisation ne devrait pas être utilisé pour gérer plusieurs utilisateurs.
3	Les applications natives Windows doivent respecter les recommandations de Microsoft et se conformer aux exigences : • du programme **Windows 7 Client Software Logo** pour Windows 7 • du « **Desktop App Certification Program** » pour Windows 8.1 cf. Certification requirements for Windows desktop apps
4	En particulier, les exigences suivantes devraient être respectées:
4.1	L'ensemble des données relatives à un utilisateur (comme le galss.ini) doivent être stockées dans Users\<username>\AppData\...
4.2	Aucun fichier ne devrait être installé directement dans le répertoire "Windows" ou l'un de ses sous répertoires
4.3	L'ensemble des fichiers exécutables doit être signé avec un certificat Authenticode
4.4	Les applications doivent supporter nativement le mode 64-bit
4.5	Les applications doivent suivre le "User Account Control (UAC) Guidelines" et inclure un fichier manifest avec un requestedExecutionLevel approprié
4.6	L'ensemble des applications doivent être compilé avec l'ensemble des mécanismes de défenses proposés par Microsoft

Tableau 164 : Guidelines logiciels Poste de travail

28Annexe – Détection d'une installation Cryptolib CPS sous Windows

<table>
<tr><th>#</th><th colspan="2">Détection d'une installation Cryptolib CPS</th></tr>
<tr><td>1</td><td colspan="2">La méthode la plus pérenne sous Windows pour détecter une installation de la Cryptolib CPS sur le poste de travail consiste à utiliser WMI pour consulter la base de données de programmes installés.</td></tr>
<tr><td rowspan="2">2</td><td>cmd</td><td><code>wmic /node:"%computername%" path WIN32_Product where "Vendor like '%ASIP%'" get * /format:csv</code></td></tr>
<tr><td>output</td><td>Exemple de sortie de cette commande:

Rem liste des propriétés disponibles:
Node,AssignmentType,Caption,Description,HelpLink,HelpTelephone,IdentifyingNumber,InstallDate,InstallDate2,InstallLocation,InstallSource,InstallState,Language,LocalPackage,Name,PackageCache,PackageCode,PackageName,ProductID,RegCompany,RegOwner,SKUNumber,Transforms,URLInfoAbout,URLUpdateInfo,Vendor,Version,WordCount

Rem sortie:
<code>[Node],1,Composants Cryptographiques CPS v5.0.8,Composants Cryptographiques CPS v5.0.8,,,{4748C15E-92F4-4FE8-BB47-6234D0CAE49B},20131213,,C:\Program Files\santesocial\CPS\,[InstallSource],5,1036,C:\Windows\Installer\5d931.msi,Composants Cryptographiques CPS v5.0.8,C:\Windows\Installer\5d931.msi,{3D1D65DD-210C-4BF4-A40C-5E725244BCF9},CryptolibCPS-v5.0.8.msi,none,,[RegOwner],,,http://esante.gouv.fr/,,ASIP Santé,5.0.8,0</code></td></tr>
<tr><td rowspan="2">3</td><td>Power Shell</td><td><code>Get-WmiObject -Class win32_product -filter "Vendor like '%ASIP%'" | Sort name | ft Name, Version, IdentifyingNumber, Vendor -Autosize</code></td></tr>
<tr><td>output</td><td>Exemple de sortie de cette commande:

<code>Name   Version IdentifyingNumber
Vendor
----   ------- -----------------

Composants Cryptographiques CPS v5.0.8 (x64) 5.0.8   {4748C15E-92F4-4FE8-BB47-6234D0CAE49B} ASIP Santé</code></td></tr>
</table>

Tableau 165 : Détection d'une installation Cryptolib CPS

29Annexe – Déclaration des cartes de santé sous Windows 7+

#	Déclaration des cartes de Santé sous Windows 7+
1	La déclaration de la carte CPx auprès des systèmes Windows 7+ est décrite dans la partie « **installation et utilisation avancée** » > « **Association manuelle de la carte CPx avec le CSP** » de ce document.
2	Lorsque qu'une carte Vitale est insérée dans un lecteur PC/SC connecté à un PC sous Windows 7+, le mécanisme d'installation de drivers de Windows est déclenché, à l'image de ce qui a été décrit plus haut pour la carte CPx (partie « **installation et utilisation avancée** » > « **Association manuelle de la carte CPx avec le CSP** ».
3	Aucun CSP n'est cependant fourni avec la carte Vitale : le mécanisme de recherche de pilote échoue.
4	La carte Vitale est utilisable mais l'utilisateur peut être perturbé par ces messages d'erreur.
5	Une solution consiste à désactiver Windows Update et l'installation automatique de dispositif (voir partie « **Windows Update** » > « **exemple de configuration simple** »)
6	Une autre solution consiste à associer un CSP « fantôme » à la carte Vitale :
7	Ces ATR peuvent être insérés en base de registre sous la clé **HKLM\Software\Microsoft\Cryptography\Calais\Smartcards** sous la valeur « **ATR** » (voir plus haut).
8	Microsoft prévoit une chaine de caractère spéciale pour associer sélectivement ces ATR à un CSP qui ne fait rien: **HKLM\Software\Microsoft\Cryptography\Calais\Smartcards** sous la valeur « **Crypto Provider** » (voir plus haut) mettre : **$DisableSCPnP$**
9	Cette méthode peut être appliquée à la CPx pour inhiber les messages d'erreurs sous Win7 64bits avec la Cryptolib CPS v4 ou la Cryptolib CPS v5 32bit, cette dernière configuration n'étant pas recommandée.
10	Cette méthode peut être appliquée aux solutions de facturations Full PC/SC déployées sous Windows si celles-ci n'intègrent pas ce paramétrage (à confirmer en test et/ou avec l'éditeur de la solution).

Tableau 166 : Déclaration des cartes de Santé sous Windows 7+

<table>
<tr><th colspan="2">Détails des déclarations des cartes de Santé sous Windows 7+</th></tr>
<tr><td>CPS</td><td><pre>
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Carte de Professionnel de Sante CPS3]
@=""
"ATR"=hex:3b,00,00,00,00,00,12,25,00,64,80,00,00,00,00,90,00
; default ASIP Santé provider:
"Crypto Provider"="ASIP Sante Cryptographic Provider"
; comment this in favor of:
;"Crypto Provider"="$DisableSCPnP$"
; !!!!!!ONLY!!!!! over x64 system installed
; with Cryptolib CPS 32b !!!!!!ONLY!!!!!
; to remove scary faulty device driver installation messages.
"ATRMask"=hex:ff,00,00,00,00,ff,ff,ff,ff,ff,ff,00,00,00,ff,ff,ff

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Carte de Professionnel de Sante CPS3 - CL]
@="";
"ATR"=hex:3b,8f,80,01,00,31,b8,64,00,00,ec,c0,73,94,01,80,82,90,00,0e
; default ASIP Santé provider:
"Crypto Provider"="ASIP Sante Cryptographic Provider"
; comment this in favor of:
;"Crypto Provider"="$DisableSCPnP$"
; !!!!!!ONLY!!!!! over x64 system installed
; with Cryptolib CPS 32b !!!!!!ONLY!!!!!
; to remove scary faulty device driver installation messages.
"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,00,00,ff,c0,ff,ff,ff,ff,ff,ff,ff,ff
</pre></td></tr>
<tr><td>Vitale</td><td><pre>
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Carte Vitale 1]
@=""
"ATR"=hex:3f,65,25,00,00,09,00,90,00
"Crypto Provider"="$DisableSCPnP$"
"ATRMask"=hex:ff,ff,ff,ff,00,ff,00,ff,ff
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards\Carte Vitale 1]
@=""
"ATR"=hex:3f,65,25,00,00,09,00,90,00
"Crypto Provider"="$DisableSCPnP$"
"ATRMask"=hex:ff,ff,ff,ff,00,ff,00,ff,ff

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Carte Vitale 2]
@=""
"ATR"=hex:3b,75,13,00,00,40,09,ea,90,00
"Crypto Provider"="$DisableSCPnP$"
"ATRMask"=hex:ff,ff,ff,ff,ff,f0,ff,ff,ff,ff
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards\Carte Vitale 2]
@=""
"ATR"=hex:3b,75,13,00,00,40,09,ea,90,00
"Crypto Provider"="$DisableSCPnP$"
"ATRMask"=hex:ff,ff,ff,ff,ff,f0,ff,ff,ff,ff
</pre></td></tr>
</table>

Tableau 167 : Détails des déclarations des cartes de Santé sous Windows 7+

30Annexe – Configuration des icônes de la barre de tâche Windows

#	Point d'attention
0010	Sous Windows 7, le « Gestionnaire de certificat CPS » (CCM) est masqué, ce qui empêche l'utilisateur de voir l'état de sa carte dans le lecteur

#	Solution
0010	Configuration du système suivant la procédure suivante

1er paramétrage: configurer la zone de notification pour que tous les icônes soient toujours visibles :

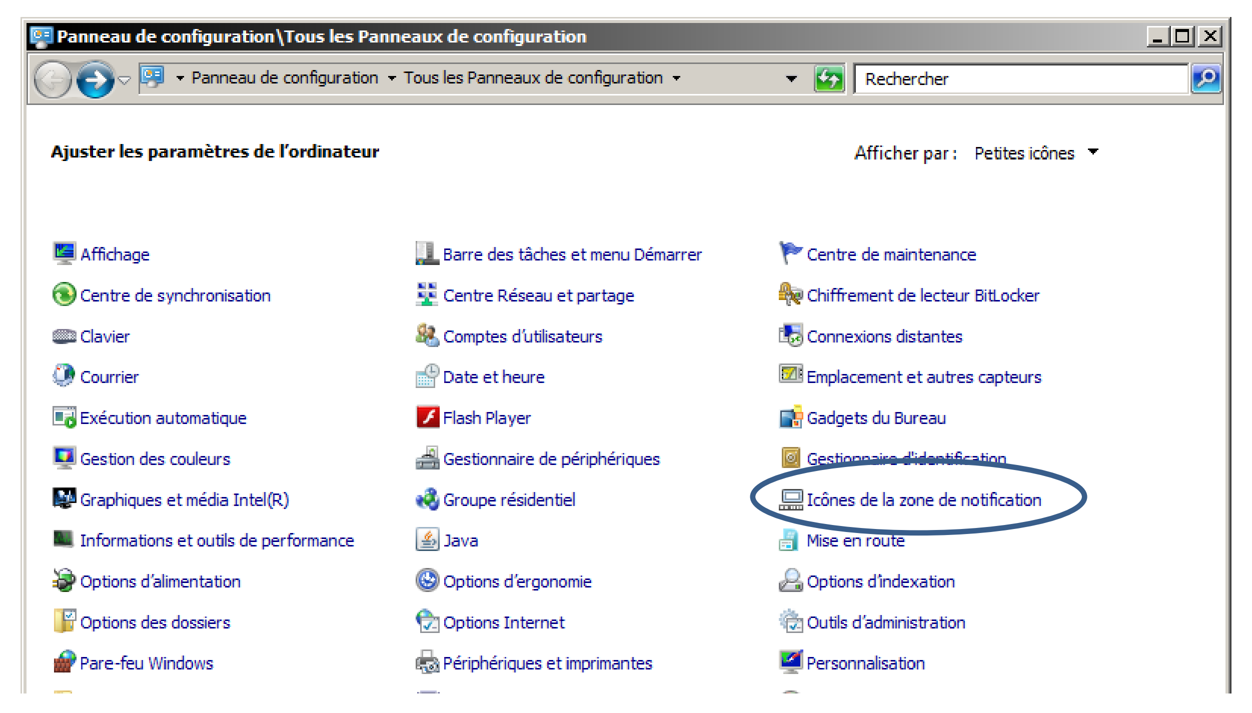


Figure 124 : Windows : Configuration : Paramétrage des icônes de la zone de configuration

La fenêtre suivante apparaît. Cocher l'option « **Toujours afficher toutes les icônes et les notifications sur la barre des tâches** » :

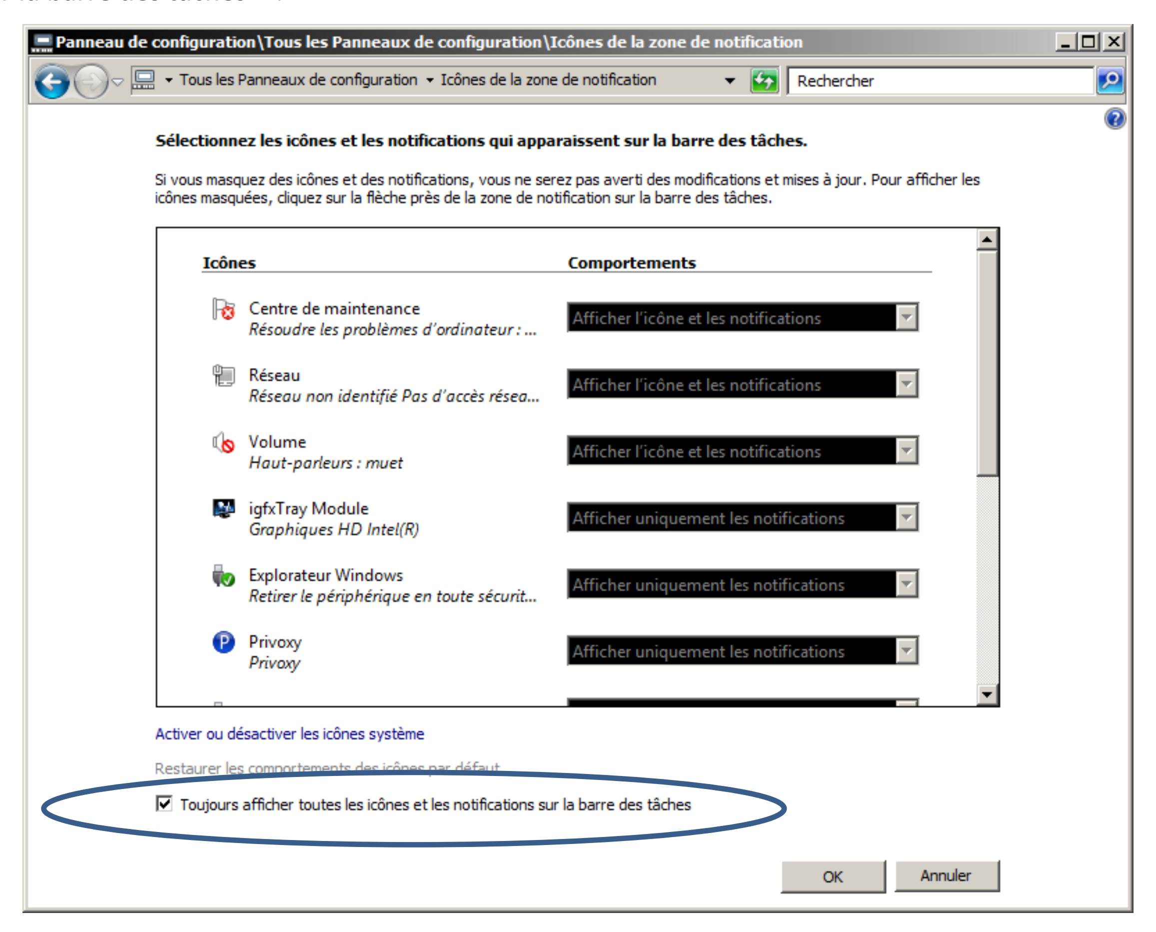


Figure 125 : Windows : Configuration : Afficher tous les icônes

Ceci permet d'avoir tout le temps sous les yeux l'état du lecteur de carte et de la carte dans le lecteur de carte :



Figure 126 : Windows : Configuration : Tous les icônes toujours visibles, dont le Gestionnaire de certificat CPS (CCM)

Cette opération peut se faire en éditant la base de registre :

Clé	[HKEY_CURRENT_USER\SOFTWARE \Microsoft\Windows\CurrentVersion\Explorer] [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]		
0001	**Valeur**	**Type**	**Valeurs possibles**
	EnableAutoTray	REG_DWORD	0 = display inactive icons 1 = hide inactive icons

Tableau 168 : Windows : Configuration : Rendre tous les icônes toujours visibles via la base de registre

Autre possibilité : configurer le Gestionnaire de certificat CPS (CCM) pour qu'il soit toujours visible:

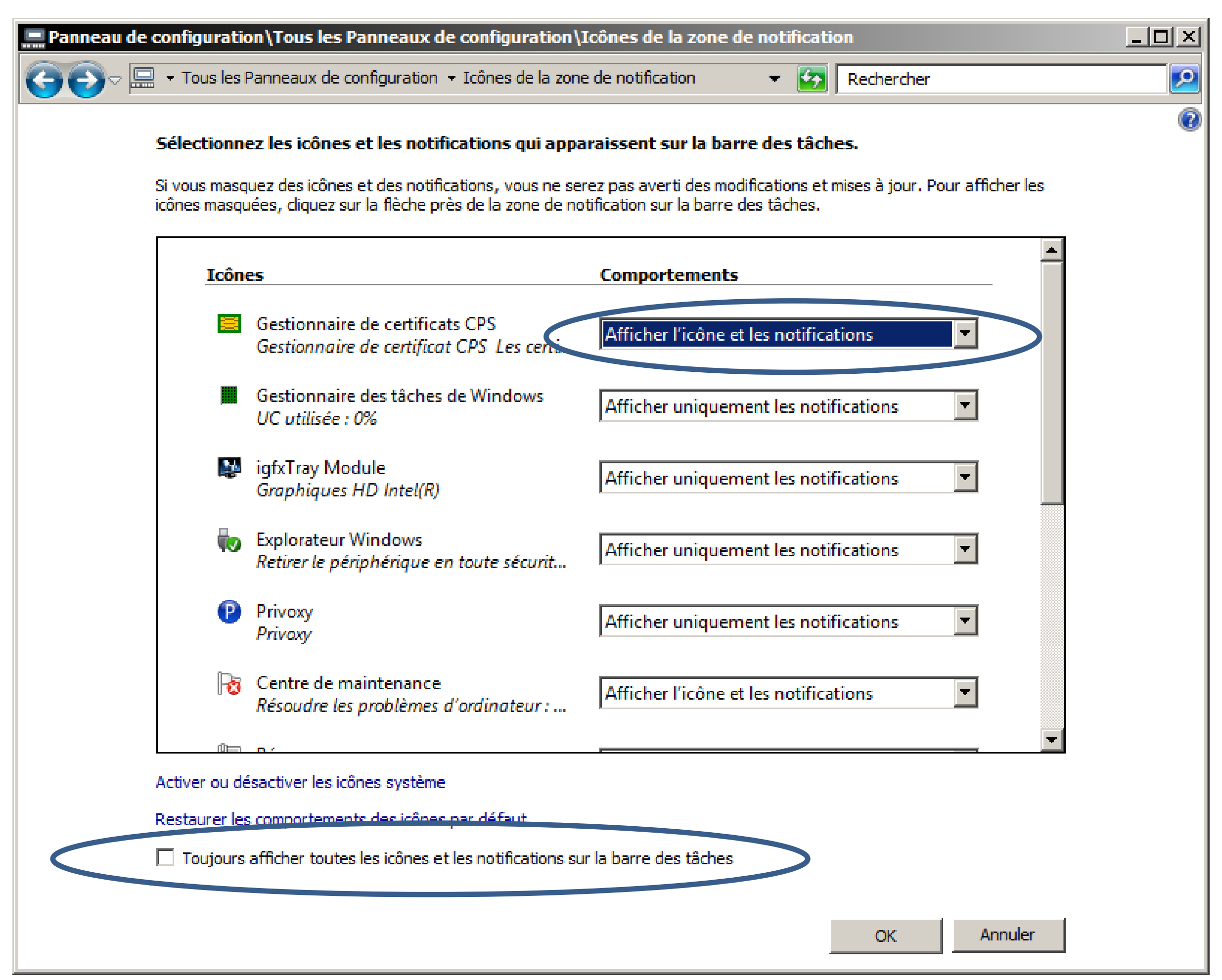


Figure 127 : Windows : Configuration : Gestionnaire de certificat CPS (CCM) toujours visible

Dans ce cas de figure, l'option « **Toujours afficher toutes les icônes et les notifications sur la barre des tâches** » reste décocher et la configuration se fait spécifiquement pour l'icône du Gestionnaire de certificats CPS en choisissant le comportement « **Afficher l'icône et les notifications** ».

31Annexe – Numéros de série de la CPx

La carte CPS3 possède trois « numéros de série »:

<table>
<tr><th>#</th><th>Identifiant</th><th>Accès</th><th>Description</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">numéro RFID :

« UID » en type A
« PUPI » en type B</td><td>En sans contact uniquement</td><td>identifiant en mode sans-contact</td></tr>
<tr><td>via une commande lecteur PC/SC v2</td><td>non publié</td></tr>
<tr><td rowspan="9">2</td><td rowspan="9">identifiant logique ou numéro de carte :

« IdCarteLog »</td><td rowspan="9">En contact uniquement</td><td>numéro à 10 chiffres</td></tr>
<tr><td>unique pour chaque carte CPx</td></tr>
<tr><td>inscrit sur le visuel, juste sous le nom du porteur</td></tr>
<tr><td>public</td></tr>
<tr><td>publié dans notre annuaire</td></tr>
<tr><td>présent dans les certificats des cartes CPx</td></tr>
<tr><td>2nde partie de l'extension privée gipCardID
cf. http://integrateurs-cps.asipsante.fr/documents/IGC-CPS2ter-2020-Certificats-X.509-et-CRL-V1.0.pdf</td></tr>
<tr><td>présent dans toutes les générations de cartes CPx</td></tr>
<tr><td>retourné par les deux librairies cps_pkcs11_w32 (v4) et cps3_pkcs11_wxx (v5) dans le champ Label de la structure TOKEN_INFO (voir tableau ci-après)</td></tr>
<tr><td rowspan="7">3</td><td rowspan="7">identifiant IAS-ECC :

« IdCarteIAS »</td><td rowspan="7">1 seul identifiant IAS-ECC accessible en contact <u>et</u> en sans contact via des APDU

(cf. [23] GIXEL IAS-ECC)</td><td>numéro sur 8 chiffres</td></tr>
<tr><td>unique pour chaque carte CPx</td></tr>
<tr><td>identifiant interne de la puce IAS</td></tr>
<tr><td>n'apparait ni sur le visuel ni dans les certificats</td></tr>
<tr><td>non publié</td></tr>
<tr><td>n'est présent que dans la carte CPS3, il n'existe pas dans la CPS2ter</td></tr>
<tr><td>retourné seulement par la librairie PKCS#11 de la Cryptolib CPS v5 (cps3_pkcs11_wxx) dans le champ SerialNumber de la structure TOKEN_INFO (voir tableau ci-après)</td></tr>
</table>

Tableau 169 : identifiants CPx

Carte	Cryptolib CPS	SerialNumber (TOKEN_INFO)	Label (TOKEN_INFO)
CPS2ter	Cryptolib CPS v4	IdCarteLog	CPS-IdCarteLog
CPS3	Cryptolib CPS v4	IdCarteLog	CPS-IdCarteLog
CPS2ter	Cryptolib CPS v5	IdCarteLog	CPS2ter-IdCarteLog
CPS3	Cryptolib CPS v5	IdCarteIAS	CPS3v1-IdCarteLog

Tableau 170 : Gestion des identifiants CPx via C_GetTokenInfo et TOKEN_INFO

32Annexe – Ecosystème CPx

Ce tableau recense les produits logiciels conçus autour de la carte CPx

#	Produits	Description
1	CleoCPS	Génération de bi-clefs de confidentialité, génération de certificat C4, révocation de certificats
2	TestSSL	Serveur de test d'authentification par carte CPx
3	ODI	Outil de Diagnostic et d'Installation
4	Outil de déblocage carte CPx	Outil en ligne sur le site sante.gouv.fr permettant le déblocage en ligne d'une carte CPx

Tableau 171 : Ecosystème CPx

33Annexe – Description de l'installeur Cryptolib CPS v5

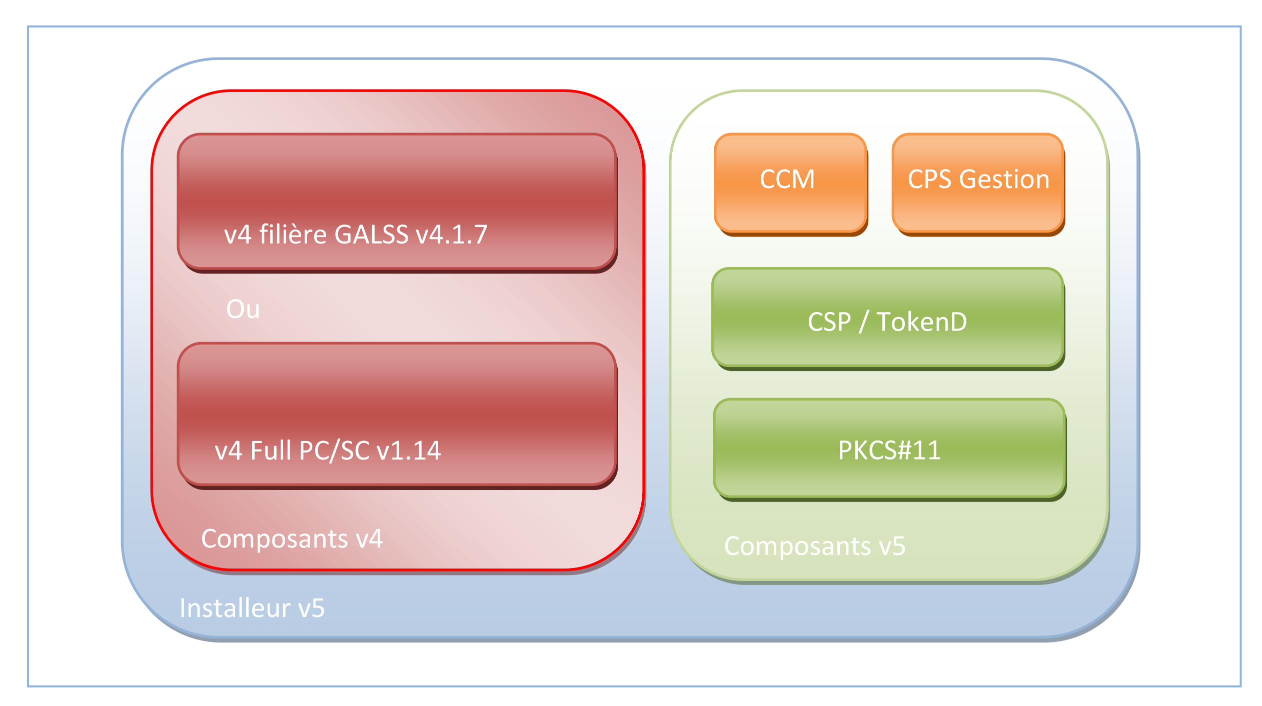


Figure 128 : description de l'installeur Cryptolib CPS v5

Par défaut, l'installeur Cryptolib CPS v5 installe les composants v5 ainsi que les composants Cryptolib CPS v4 GALSS :

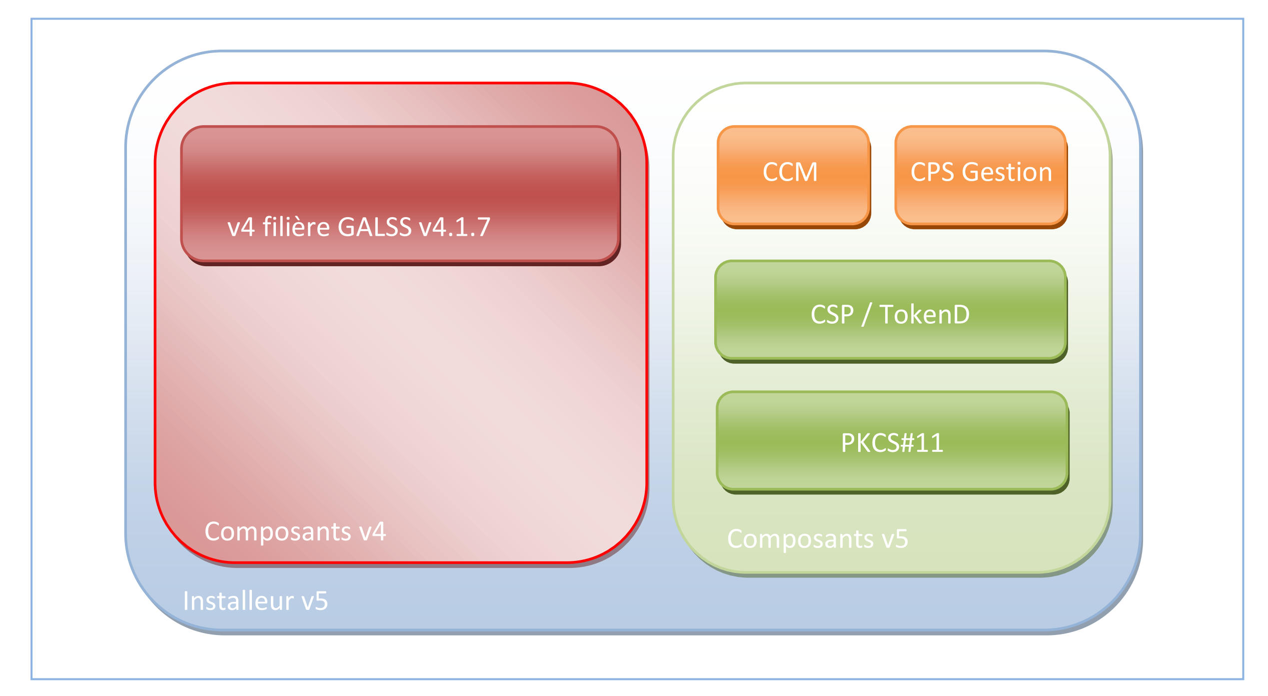


Figure 129 : résultat de l'installation de la Cryptolib CPS v5 par défaut

Ceci permet notamment d'assurer qu'une application fonctionnant avec les composants v4 fonctionnera toujours après installation de la Cryptolib CPS v5.

34Annexe – ODI

Chaque version d'ODI (MSSanté, DMP, générique) est accompagnée d'une FAQ accessible depuis un navigateur Web et qui recense les questions, problèmes et contournements connus.

34.1 Gestion cache Java

ODI a besoin que le cache Java soit activé pour fonctionner :

#	Description
1	« Panneau de configuration »
2	« Java » ou « Java (32bits) »
3	« Général »
4	« Fichiers Internet Temporaires »
5	« Paramètres… »
6	S'assurer que « Stocker les fichiers temporaires sur mon ordinateur. » est coché
7	S'assurer que la quantité d'espace disque allouée au stockage des fichiers temporaires est suffisante (quelques dizaines de MB pour ODI suffisent)
8	En cas d'instabilités constatées avec ODI, vider le cache java en :
9	Cliquant sur « Supprimer les fichiers… »
10	Cochant « Applications et applets installées » en plus de « Fichiers traces » et « Applications et applets en mémoire cache »
11	Cliquer sur « OK »

Tableau 172 : ODI : Gestion Cache Java

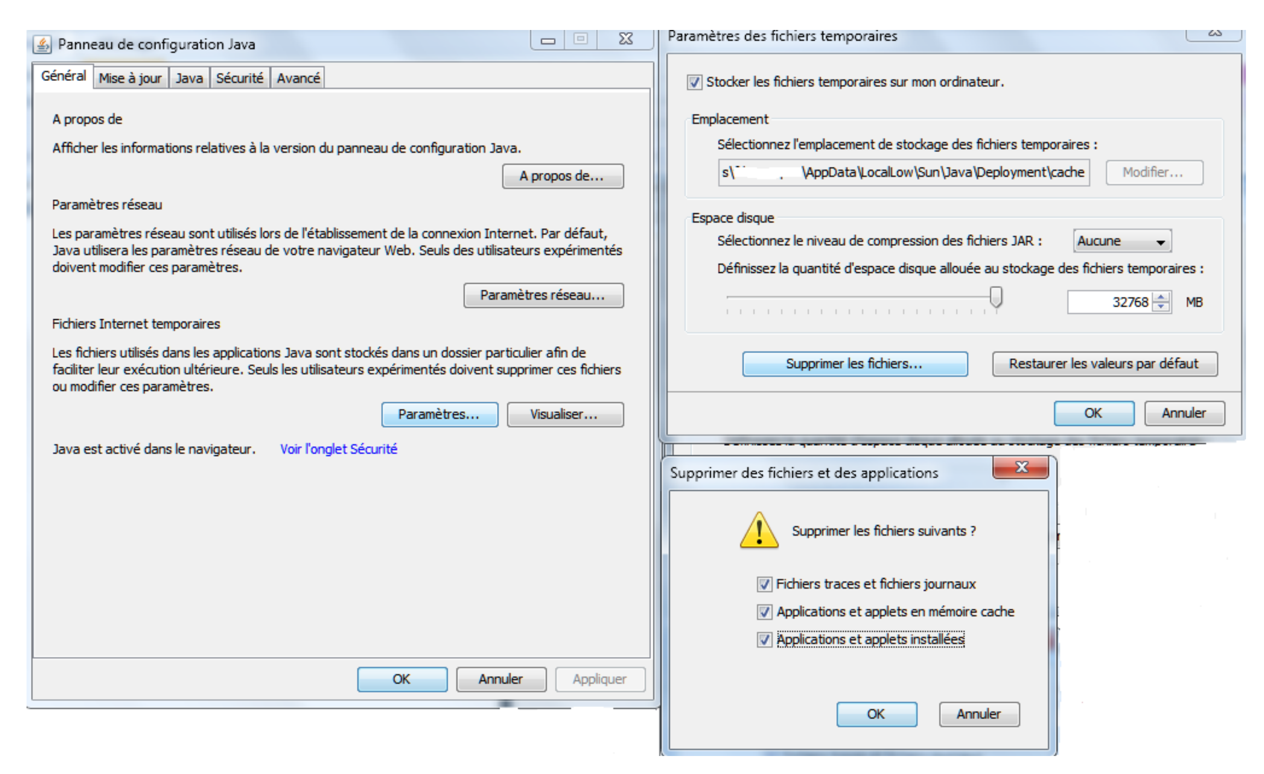


Figure 130 : ODI : Gestion cache Java



35Annexe – Ecarts d'implémentation CSP / CryptoAPI

API	Disponibilité CSP	Disponibilité ASIP	CSP CPS3 v2.10.0 (Cryptolib CPS 5.0.13)	CSP CPS3 v2.11.0 (Cryptolib CPS 5.0.15)
CPAcquireContext	Requise	Implémenté		
CPCreateHash	Requise	Implémenté		
CPDecrypt	Requise	Implémenté		
CPDeriveKey	Requise	Non implémenté	Génère une clé de session à partir d'un condensat pré-calculé	
CPDestroyHash	Requise	Implémenté		
CPDestroyKey	Requise	Implémenté		
CPEncrypt	Requise	Implémenté		
CPExportKey	Requise	Implémenté		
CPGenKey	Requise	Non implémenté	Génère une clé de session ou une bi-clé RSA aléatoire.	
CPGenRandom	Requise	Implémenté		
CPGetHashParam	Requise	Implémenté		
CPGetKeyParam	Requise	Implémenté avec écarts	valeurs non prises en compte de **dwParam**: KP_SALT, KP_PERMISSIONS KP_IV, KP_PADDING, KP_MODE, **KP_KEYLEN**	valeurs non prises en compte de **dwParam**: KP_SALT, KP_PERMISSIONS KP_IV, KP_PADDING, KP_MODE, **KP_KEYLEN (Google Chrome 41)**
CPGetProvParam	Requise	Implémenté avec écarts	valeurs non prises en compte de **dwParam**: PP_PROVTYPE , PP_KEYSPEC, PP_SMARTCARD_READER, PP_SMARTCARD_GUID , PP_USE_HARDWARE_RNG , PP_KEYSET_TYPE	valeurs non prises en compte de **dwParam**: PP_PROVTYPE , PP_KEYSPEC , PP_SMARTCARD_READER, PP_SMARTCARD_GUID , PP_USE_HARDWARE_RNG , PP_KEYSET_TYPE
CPGetUserKey	Requise	Implémenté		
CPHashData	Requise	Implémenté		
CPHashSessionKey	Requise	Non implémenté	Permet de hasher une clé de session dont le handle est passé en paramètre	
CPImportKey	Requise	Implémenté		

API	Disponibilité CSP	Disponibilité ASIP	CSP CPS3 v2.10.0 (Cryptolib CPS 5.0.13)	CSP CPS3 v2.11.0 (Cryptolib CPS 5.0.15)
CPReleaseContext	Requise	Implémenté		
CPSetHashParam	Requise	Implémenté		
CPSetKeyParam	Requise	Implémenté avec écarts	valeurs non prises en compte de **dwParam**: KP_SALT, KP_PERMISSIONS, KP_PADDING, KP_MODE, KP_KEYVAL	valeurs non prises en compte de **dwParam**: KP_SALT, KP_PERMISSIONS, KP_PADDING, KP_MODE, KP_KEYVAL
CPSetProvParam	Requise	Implémenté avec écarts	valeurs non prises en compte de **dwParam**: PP_SIGNATURE_PIN (eq. PP_EXCHANGE_PIN), PP_USE_HARDWARE_RNG , PP_SMARTCARD_READER, PP_SMARTCARD_GUID	valeurs non prises en compte de **dwParam**: PP_SIGNATURE_PIN (eq. PP_EXCHANGE_PIN) PP_USE_HARDWARE_RNG PP_SMARTCARD_READER PP_SMARTCARD_GUID
CPSignHash	Requise	Implémenté		
CPVerifySignature	Requise	Implémenté		
CPDuplicateHash	Optionnelle	Non implémenté		
CPDuplicateKey	Optionnelle	Non implémenté		

Tableau 173 : Ecarts d'implémentation CSP / CryptoAPI



36Annexe – Points d’attention et contournements

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0010		Win7	x64	Sous Win7 64b, si l’UAC est positionné à un niveau différent de « désactivé » et que l’EPM est activé, IE10+ passe en mode 64b. Des erreurs « carte absente » peuvent alors apparaître en authentification SSL par exemple.	La Cryptolib CPS v5 64b est alors requise pour que le CSP 64b soit chargé. Si la carte CPx est insérée dans un lecteur PSS, il faut aussi un GALSS 64b pour IE puisse utiliser la carte.	Confirmé	Confirmé
AT_0020		Win8 Win8.1	x86 x64	La Cryptolib CPS ne fonctionne pas avec Internet Explorer en interface Metro.	Utiliser Internet Explorer en interface desktop.	Confirmé	Confirmé
AT_0030		Win7 Win8 Win8.1	x64	Le CCM et CPS-Gestion installés par la Cryptolib CPS 64b sont des applications 64b. Ils ne fonctionnent pas si la carte CPx est insérée dans un lecteur PSS (en attente du GALSS 64b).	Au choix : 1. Installer la Cryptolib CPS 32b 2. Mettre la carte CPS dans un lecteur PC/SC. 3. Installer le GALSS 64b 4. Utiliser le CCM et CPS-Gestion 32b prélevés dans l’installeur Cryptolib CPS 32b	Confirmé	Confirmé

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0040	0000882	Win8 Win8.1	x86 x64	Internet Explorer en interface desktop ne fonctionne pas avec une carte CPS insérée dans un lecteur PSS si l'EPM est activé.	Ceci est dû à une limitation du GALSS. Au choix : 1. Mettre la carte CPS dans un lecteur PC/SC. 2. Ajouter le site courant à la liste des sites de confiance. 3. Désactiver l'EPM 4. Installer le KB2888505	Confirmé	Confirmé
AT_0050	0001122	Toute plate-forme	x86 x64	Les accès au fichier **galss.ini** effectués par le GALSS et la Cryptolib CPS sont trop fréquents, entrainant des problèmes de performances.	Eviter la distribution du galss.ini via le réseau local ou les profils itinérants.	Confirmé	N/A
AT_0060		Mac OS X		Le fichier **reader.conf** n'est pas copié à l'installation si le GALSS n'est pas installé du fait d'une limitation de pcscd sous Mac OS X : https://smartcardservices.macosforge.org/trac/ticket/40 La présence de ce fichier **reader.conf** sans avoir de lecteur PC/SC branché fait « crasher » PC/SC.	Le problème affecte les Mac équipés de lecteurs PSS. L'alternative consiste à s'assurer que le fichier **reader.conf** n'existe pas, ou si il existe, de le renommer en **reader.gip**	Confirmé	Confirmé

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0070	0001047			**Env. Citrix :** Les transactions carte à puce mal fermées peuvent affectées les sessions courantes et empêcher la création de nouvelles sessions en contexte Citrix.	Corrigé par Citrix, se référer à http://support.citrix.com/article/CTX136248 http://support.citrix.com/article/CTX136922 Section « Smartcard » et appliquer les clefs : **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard** Name: **TransactionTimeoutEnable** Type: REG_DWORD Value: 1 (enable) **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard** Name: **TransactionTimeoutValue** Type: REG_DWORD Value: <any value more than 5 seconds> **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard** Name: **SendRecvTimeout** Type: REG_DWORD Value: Minimum timeout value, in seconds; should be 30 seconds or more. Any lesser value defaults to 30 seconds. This value must be at least 10 seconds less than "TransactionTimeoutValue". **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SmartCard** Name: **SupLowIntegrityProc** Type: REG_DWORD Data: 1 **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard** Name: **SupLowIntegrityProc** Type: REG_DWORD Data: 1	Clos	Confirmé

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0080	0013450	**WinXP Win2003**	**x86 x64**	Les OS à base de noyau XP ne sont pas nativement compatibles avec la nouvelle architecture cryptographique Microsoft.	L'installation du KB909520 (Base CSP pour noyaux XP) sera requise à terme.	Confirmé	Confirmé
AT_0090	0013451	**WinXP Win2003**	**x86 x64**	L'OS Win XP ne sera plus supporté par Microsoft à partir d'avril 2014. A partir de cette date, Microsoft ne supportera plus l'actuel processus de signature des CSP. Les futures Cryptolib CPS seront donc signées par Authenticode uniquement.	Afin de faire fonctionner la Cryptolib CPS sur Win XP, il sera nécessaire d'installer le KB2836198 (Authenticode Signing for CSP signatures)	Confirmé	Confirmé
AT_0100	0001129	**Windows**	**x86 x64**	Il n'est pas possible de faire du SHA256 au niveau CSP sous Windows.	Ceci est dû au fait que le CSP est de **type 1 (PROV_RSA_FULL)** et non de **type 24 (PROV_RSA_AES)**. Pour faire du SHA256 : passer au niveau PKCS#11 ou PC/SC.	Confirmé	Confirmé

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0110		**Windows**	**x86** **x64**	Sous Windows 7+, les messages « pilote de carte à puce non trouvé » s'affichent : • Sous Windows 7 x86, si la Cryptolib CPS v4 (32b) est installée ○ La Cryptolib CPS v4 n'associe pas les ATR des cartes CPx au CSP • Sous Windows 7 x64, si la Cryptolib CPS v4 (32b) ou si la Cryptolib CPS v5 32b sont installés ○ Dans ces cas, aucun CSP « natif / 64b » n'est installé	Pour éviter ces messages : 1. si Cryptolib CPS v4 sur Windows 7 32b : déclarer le mapping ATR manuellement (non testé, pas de support du sans contact) 2. désactiver Windows Update et le Device Search 3. installer la Cryptolib CPS v5 dans sa version destinée à l'architecture de l'OS courant (solution préconisée) 4. Déclarer un CSP « fantôme » (cf. Annexe Carte Vitale)	Confirmé	Confirmé
AT_0120		**Win8**	**x86** **x64**	Les performances avec Internet Explorer en interface desktop avec EPM activée peuvent être dégradées. Les traces/logs sont incomplètes.	Mauvais droits sur %PUBLIC%\AppData\santesocial\cps\cache\ et %PUBLIC%\AppData\santesocial\cps\log\	Clos	Corrigé avec la Cryptolib CPS v5.0.13
AT_0130		**Win7** **Win8** **Win8.1**	**x64**	Problèmes de signatures des pilotes lecteurs PSS (signatures expirées)	Re-signer les drivers Désactiver le contrôle des signatures de drivers (déconseillé)	Confirmé	Confirmé

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0140		**Mac OS X 10.10**	**x64**	20140912 : Incompatibilité avec Mac OS X 10.10 détectée avec la première version beta, sans doute du fait de l'abandon de TokenD / CDSA au profit de **Crypto Token Kit**	Nouvelle version de la Cryptolib CPS v5 pour Mac OS X en cours de développement	Confirmé	Confirmé
AT_0150		**Tous**	**x86** **x64**	La vérification de signature des certificats ASIP Santé issus de l'IGC CPS2ter (certificats présents dans les cartes CPx) ne fonctionne pas avec BouncyCastle. Lors de la vérification de signature, BouncyCastle réécrit la séquence DER et vérifie la signature sur la base de cette réécriture. Les certificats ASIP Santé n'étant pas DER-compliant (l'ordre des RDN est fixe alors que la norme X690 prévoit autre chose), la reconstruction donne un tableau de bytes différents de ce qui a été signé par l'IGC de Santé et donc la vérification de signature échoue.	Ne pas passer par de fonctions BouncyCastle utilisant DERSequence::writeObject Isoler la vérification de signature des certificats ASIP Santé dans une portion de code ne faisant pas appel à BouncyCastle	Clos	Confirmé

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0160		**Tous**	**x86 x64**	Mozilla Firefox ne détecte pas la carte CPS. La connexion par carte sur un frontal web requérant une carte CPS ne fonctionne pas avec Firefox.	Installer le .XPI « Module de sécurité CPS » depuis http://testssl.asipsante.fr/ Ré-installer la Cryptolib CPS S'assurer que le module de sécurité CPS n'a pas été désactivé (« options>modules>extensions>Activer »)	Clos	Confirmé
AT_0170		**Tous**	**x86 x64**	Une erreur a lieu systématiquement lors de la signature de documents avec une CPS insérée dans un lecteur PSS alors que le reste des fonctionnalités carte fonctionnent.	S'assurer que le reste des fonctionnalités carte fonctionnent effectivement et que les problèmes sont cantonnés à la signature électronique de documents avec un lecteur PSS. Mettre à jour le logiciel lecteur (des problèmes ont été détectés avec l'OS 1.15 et l'application 3.02 sur Prium 3S, réglés en passant sur 1.19 et 3.04 par ex.)	Clos	Clos
AT_0180		**Windows**	**x86 x64**	Une erreur a lieu en authentification web avec Chrome 41 et la Cryptolib CPS v4 ou la Cryptolib CPS v5 5.0.13	L'erreur est liée à une évolution de Chrome 41 qui demande désormais la taille de clé d'authentification utilisée au CSP. Le CSP n'implémentait pas cette fonctionnalité. Les alternatives sont donc : changer de navigateur ou passer à la Cryptolib CPS v5.0.15+	Clos	Corrigé avec la Cryptolib CPS v5.0.15

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0190		**Windows**	**x86** **x64**	Le CSP Cryptolib CPS v5 n'implémente pas toutes les API de CryptoAPI. Les applications Windows s'intégrant avec la carte au niveau CSP ne peuvent donc pas utiliser toutes les fonctions proposées par CryptoAPI	Prendre connaissance des écarts de la v5.0.15+ vis-à-vis de CryptoAPI et éviter d'utiliser les appels concernés (cf. Annexe – Ecarts d'implémentation CSP / CryptoAPI) Attendre la sortie d'une version du CSP plus complète S'intégrer au niveau PKCS#11	Confirmé	Confirmé
AT_0200		**Tous**	**x86** **x64**	Sur une infrastructure client-serveur dans laquelle le serveur utilise une version de OpenSSL 1.0.1k ou supérieure, l'authentification Web par carte CPx est impossible avec des cartes CPx produites avant octobre 2014. Les erreurs de connexion côté client sont accompagnées de logs d'erreur d'OpenSSL « invalid bit string bits left » côté serveur.	OpenSSL 1.0.1k ou supérieure est sensible à une non-conformité des certificats CPS vis-à-vis de la norme X.509. OpenSSL rejette les certificats non conformes suite à la publication de la CVE-2014-8275 (https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8275). 2 alternatives : - Patcher OpenSSL (voir site integrateurs-cps.asipsante.fr) - Installer une version récente de la Cryptolib CPS	Clos	Corrigé avec la Cryptolib CPS v5.0.15 (Windows), 5.0.15 (Mac OS X) ou 5.0.7 (Linux) Corrigé avec un patch OpenSSL dédié coté Serveur

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0210		**Windows**	**x86** **x64**	La mise en œuvre du code exemple C# génère des messages « carte absente » en Cryptolib CPS 5.0.13, 5.0.15, 5.0.16 et 5.0.17	- Sélectionner le certificat ASIP Santé pour l'usage souhaité en utilisant le filtre proposé par l'objet X509Certificate2Collection comme illustrer dans ce document - Passer sur la Cryptolib CPS 5.0.18+	Clos	Corrigé avec la Cryptolib CPS v5.0.18 (Windows)
AT_0220		**Windows 10**	**x86** **x64**	La Cryptolib CPS ne fonctionne pas avec le nouveau navigateur Spartan/Edge fourni par Microsoft avec les versions « preview » de Windows 10 : avec ce navigateur, sous cet OS, les authentifications Web par carte CPS ne fonctionnent pas	- Rebasculer sous IE11 : avec IE11, fourni parallèlement aussi sous cet OS, la Cryptolib CPS fonctionne (cf. IE11 sous Windows 10 plus bas) - D'autres impacts sont à prévoir sous cet OS (nécessité d'avoir une filière full 64bits, abandon du support de VBScript, d'ActiveX, de Java, nouveau User-Agent…) (cf. Cryptolib CPS et Edge plus bas)	Clos	Corrigé avec la Cryptolib CPS v5.0.19+ et les lecteurs PC/SC (Windows)

Tableau 174 : Points d'attentions et contournements



37Annexe – Choix de lecteur

Compte-tenu des spécificités Santé&Social (PSS, pas de GALSS 64b, Cryptolib CPS 64b en v5 seulement, sans-contact, Smartcard Logon seulement avec les PC/SC…), le choix d'un lecteur de carte peut être un peu compliqué quand on part de zéro.

La question du choix de lecteur est donc une question récurrente.

Etant entendu que l'ASIP Santé ne préconise de lecteurs (ni terme de types ni en terme de fabricants/modèles), l'ASIP Santé oriente les choix en rappelant :

1. Les critères de conformités vis-à-vis de standards internationaux reconnus (PC/SC, USB, CCID)
2. Les critères de support (fabricants de lecteur, OS)
3. Les critères de grille de compatibilité (support éditeurs, grilles de compatibilité des services ASIP Santé, qui dans ce cas joue le rôle d'éditeur / intégrateur)
4. Les critères de tests (test de logiciels vis-à-vis de lecteurs particuliers / veille)
5. Les critères de coûts d'acquisition et de possession

La question du « choix de lecteur » est souvent un « faux problème » au niveau projet sachant que le parc visé est assez souvent déjà pré-équipé en lecteurs.

Elle mérite cependant d'être isolée pour pouvoir « challenger » un projet donné à un moment donné:

- « si le projet devait être déployé sur un parc de PDT sans lecteur de carte, lequel choisirait-il » ?
- « si le projet devait être déployé sur un parc de PDT équipé de lecteur de carte, fonctionnerait-il avec ces lecteurs » ?

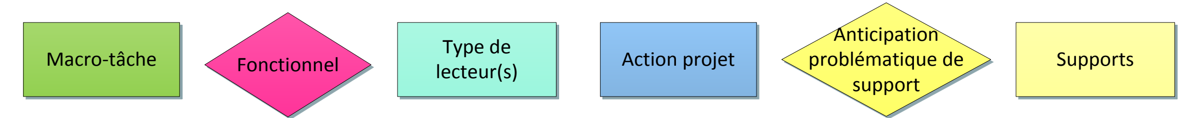
Et permet donc de vérifier la bonne compréhension technique de la gestion du parc de lecteur induite.

Dans le cas où le déploiement de PC/SC est possible (établissements), les coûts d'acquisition et de possession de lecteurs PC/SC ainsi que la couverture technique offerte (64b, TSE, mode protégé renforcé, sans-contact, Smartcard logon) devrait être systématique.

Les schémas ci-après visent à :

- orienter les choix vers des standards reconnus
- sortir le support ASIP Santé de ces problématiques, l'ASIP Santé n'assurant pas de support lecteur (ni PSS, ni PC/SC ni déploiement)
- orienter les chefs de projets vers les recherches de niveau de support OS/fabriquant/éditeur et GIE SV pour qu'ils organisent leur support en conséquence.

La prise en compte de la problématique lecteurs dans un projet Santé&Social doit suivre la logique générale suivante:



Préconisation: utilisation de standards du marché: USB, PC/SC, CCID

Figure 131 : Choix de lecteur : Légende

Projet mettant en jeu des cartes Santé&Social

Gestion des lecteurs

Types de poste client visés?

Parc de postes de travail sans lecteurs pré-installés: gestion du déploiement de lecteurs à choisir dans le périmètre projet

Parc de postes de travail avec lecteurs pré-installés

Inventaire lecteurs

Vérification que les lecteurs correspondent au fonctionnel visé

lecteurs en parc répondent au fonctionnel visé?

non

oui

Choix de lecteurs « type » correspondant au fonctionnel visé

oui

Vérification des niveaux de support (OS, GIE-SV, fabricants de lecteurs, éditeurs logiciels/LPS)

Niveaux de supports adéquates / assumables?

non

Achats

non

Déploiements

non

Organisation du support lecteurs

Figure 132 : Choix de lecteur : Logique générale de prise en compte de la problématique lecteur dans un projet Santé&Social



Cette logique permet d'aborder et de régler immédiatement toutes les questions liées au support :

Figure 133 : Choix de lecteur : Organisation des supports

Ainsi que la question particulière du choix de lecteurs PC/SC :

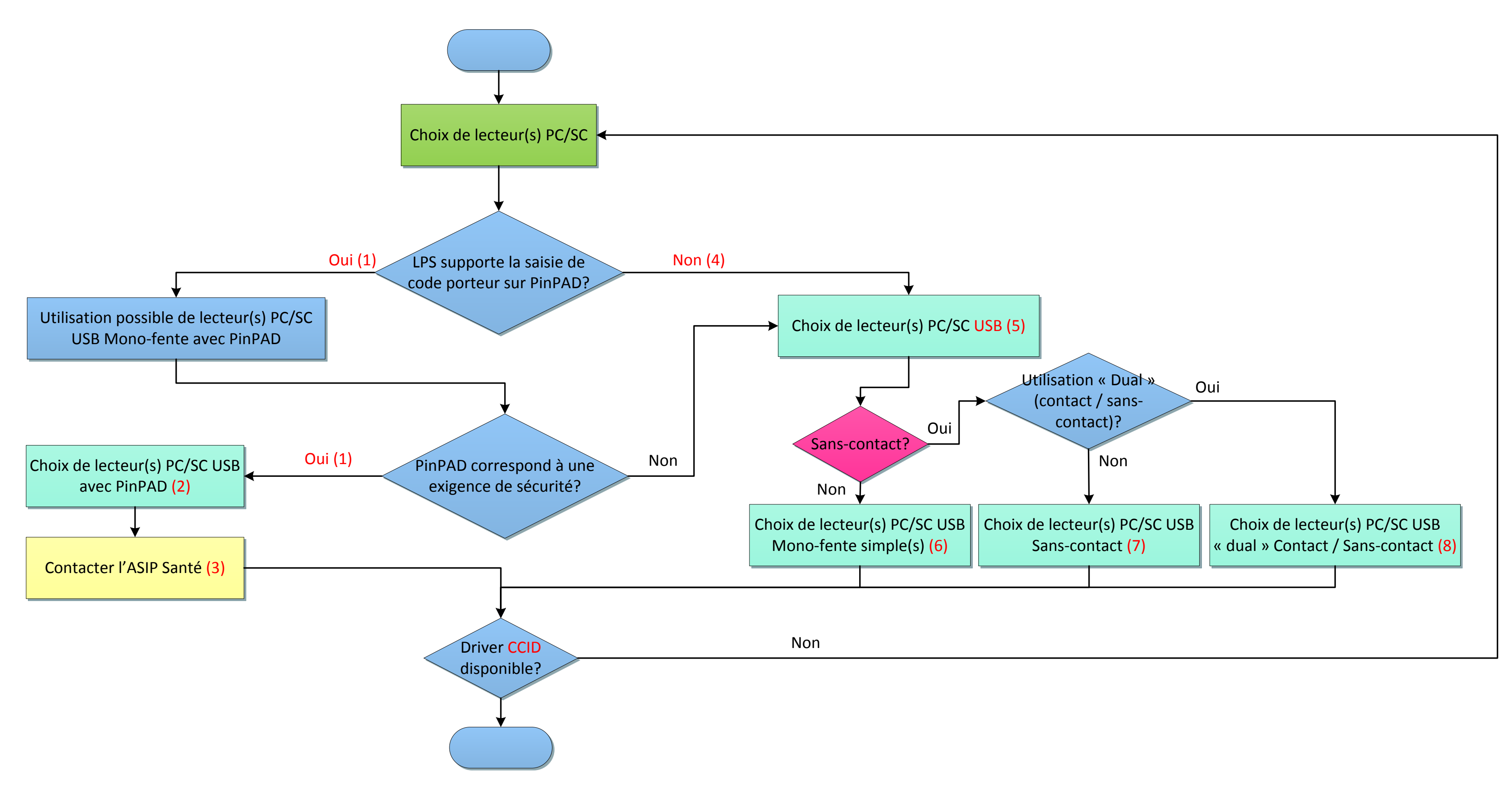


Figure 134 : Choix de lecteur PC/SC



Les questions du choix d'un lecteur à destination d'un parc de postes non équipés s'aborde en analysant le service à déployer :

Choix d'un lecteur de carte à puce par rapport à un « fonctionnel » visé
PSS
PC/SC
TLA?
Oui
Combiné Paiement CB et lecture cartes Santé&Social?
Oui
MAJ Vitale
Oui
Facturation SV?
Oui
MSSanté
DMP
CertDC E-Fit E-DO ...
TLSi
Authent. navigat.
Oui
Paiement CB seul?
Autres fonctionnalités
Smartcard logon CPS?
Oui
ModernUI?
Non
Sans-contact?
64bits?
Oui
TSE
Analyse des fonctionnalités du LPS
Non
Non
LPS supporte la Facturation SV en OT?
Oui
Choix de lecteur(s) PSS USB
Choix de lecteur(s) PC/SC
Vérification des niveaux de support (OS, GIE-SV, fabricants, éditeurs logiciels/LPS, intégrateurs)
Niveaux de supports adéquates / assumables?
Non
Oui
Tests
Tests OK?
Non
Oui
Organisation des déploiements
Organisation du support
Problèmes lecteurs / Evolution gestion lecteurs
Run

Figure 135 : Choix de lecteur : Choix en fonction du service à déployer

Si les services à déployer sont multiples, il faut reparcourir l'arbre de décision afin de détecter toute incompatibilité avec des choix faits en se concentrant sur les fonctionnalités analysées précédemment.



A l'inverse, la vérification de la compatibilité d'un lecteur donné pour une fonctionnalité donnée se fait suivant la logique générale suivante :

Figure 136 : Choix de lecteur : Vérification de l'adéquation du lecteur avec le service à déployer

Cet arbre de décision venant compléter le précédent, l'un et l'autre contribuant à « challenger » la compréhension de la situation « lecteur ».



#	Catégorie	Remarque
	support lecteur PSS Série	Le support des lecteurs PSS série est arrêté. Les configurations PC ou Mac récentes n'embarquent généralement plus de port série.
1	support lecteur PC/SC avec PinPAD	Aucune solution logicielle Santé&Social ne supporte actuellement la saisie du code porteur sur le PinPAD
2	support lecteur PC/SC avec PinPAD	Les lecteurs PC/SC avec PinPAD sont plus chers que les lecteurs PC/SC USB « simples ».
3	support lecteur PC/SC avec PinPAD	Les éditeurs désireux d'offrir la saisie du code porteur CPx sur le PinPAD sont invités à se faire connaître auprès de editeurs@asipsante.fr
4	support lecteur PC/SC USB	La majorité des logiciels gérant les lecteurs PC/SC n'utilise pas le PinPAD. Ces lecteurs sont tous USB.
5	support lecteur PC/SC USB	Les lecteurs PC/SC sans PinPAD sont peu onéreux (7€ pour un lecteur Navigo)
6 **7** **8**	support lecteur PC/SC USB	Les lecteurs PC/SC USB peuvent être mono-fente (contact), sans-contact ou dual « contact / sans-contact »). Les lecteurs dual coutent environ 90€. Le choix se fait par analyse des fonctionnalités visées ou par anticipation des fonctionnalités à venir.

Figure 137 : Choix de lecteur : remarques

38Annexe – Utilisations de Edge et de IE11 sous Windows 10

38.1 Situation

Microsoft distribuera son nouvel OS Windows 10 à partir du 29/07/2015.

Cet OS **embarquera**, qui plus est, un **nouveau navigateur** appelé « **Edge** » (jusqu'à présent son nom était « **Spartan** », d'où la double nomenclature dans ce qui suit) dont la **technologie** est **annoncée** par Microsoft comme étant en **rupture** avec celle de **Internet Explorer** (**IE)**.

Windows 10 contiendra cependant aussi **Internet Explorer 11 (IE11)**.

Cet OS sera **gratuit** en **mise à jour** depuis Win7, Win 8, Win 8.1 et Win 8.1 Update 1.

Il sera aussi **diffusé** par les **vendeurs** de matériels informatiques en tant **qu'OS par défaut** des PC neufs.

Dès lors, le parc d'OS sous Windows du secteur Santé&Social (principalement les PS libéraux) commencera à migrer vers Windows 10 progressivement.

10 points d'attention pour le **support** de ce **nouveau couple OS/navigateur** sont d'ores et déjà **identifiés** :

Ce nouvel OS a été testé par l'ASIP Santé dans ses versions beta dès sa sortie en beta (déc. 2014).

L'ASIP Santé a repris ses tests en veille technologique à l'occasion de la sortie de la beta 10130. Lors de cette reprise des tests, ont été constatés :

1. que Spartan/Edge sera le navigateur par défaut de Windows 10
    a. l'utilisateur accède difficilement (utilisateur avancé/averti) au IE11 fourni avec ce nouvel OS
2. que la Cryptolib CPS v5 **5.0.16** ne fonctionne pas telle qu'elle est fournie avec ce nouveau navigateur
    a. l'authentification Web par carte CPx ne fonctionne pas avec les versions inférieures ou égales à la 5.0.16.
3. que la Cryptolib CPS v5 fonctionne cependant avec IE 11
    a. bémol : ce n'est pas le navigateur par défaut de cet OS et l'utilisateur y accède difficilement (utilisateur avancé/averti) au IE11 fourni avec ce nouvel OS (cf. point précédent)
4. que,Spartan/Edge est lancé en 64bits sur un OS 64bits
    a. il faut s'attendre à ce que la version 32bits de cet OS soit peu distribuée
    b. la filière 64bits d'accès aux cartes complète est requise (Cryptolib CPS 64b, GALSS 64b, API de lecture 64b) pour l'accès aux cartes
5. que Spartan/Edge ne supporte pas (encore) les extensions
    a. en particulier l'extension Java : les applets ne fonctionnent pas sur ce navigateur
    b. les sites web à base d'applet ne seront plus fonctionnels
6. que Spartan/Edge intègre un plugin Flash activé par défaut
    a. les lectures de vidéos sont donc OK sur les principaux portails Santé&Social en particulier
7. que Spartan/Edge intègre effectivement un nouveau moteur de rendu
    a. cela implique pour les éditeurs de solutions logicielles basées sur un navigateur de faire des tests sur tous les services utilisant HTML pour assurer une non-régression des rendus graphiques

8. que Spartan/Edge expose aux serveurs web une nouvelle chaine de caractère « User-agent »
    a. cette chaine expose Spartan/Edge en tant que navigateur Safari ou Chrome
    b. l'ensemble des serveurs ou des codes clients (Javascript, CSS conditionnels) exploitant cette chaine de caractère sont impactés puisqu'en l'état ils risquent de prendre Edge pour un Chrome...
    c. ce type d'erreur a déjà été rencontré sur les services Santé&Social lors du passage de IE10 à IE11
9. Spartan/Edge n'a pas par défaut les droits d'accès à l'interface réseau locale (« loopback » / « localhost »)
    a. "Microsoft Edge runs with network isolation by default for security reasons."
    b. Ceci rend en particulier le service SrvSVCNAM, qui « tourne » sur cette interface, inopérant
    c. Un contournement existe mais il dégrade la sécurité de l'OS : une analyse de risque et d'impact pour les PS seront nécessaires
        i. Entrer la commande suivante: **CheckNetIsolation LoopbackExempt -a -n=Microsoft.Windows.Spartan_cw5n1h2txyewy**
    d. Dans le futur, il sera sans doute possible d'activer l'interface localhost en utilisant **about:flags**, ce qui requiert tout de même a priori l'intervention du PS.
10. Les autres points notables concernent les abandons des supports suivants :
    a. Abandon des « document modes » (quirk mode / standard mode)
    b. Abandon de la Chaine X-UA-Compatible (mode compatibilité)
    c. Abandon du VBScript
    d. Abandon des anciennes manières d'utiliser currentStyle et attachEvent (impact sur les vieux Javascript)

38.2 IE11 sous Windows 10

Afin d'utiliser IE11 sous Windows 10, les manipulations suivantes sont nécessaires :

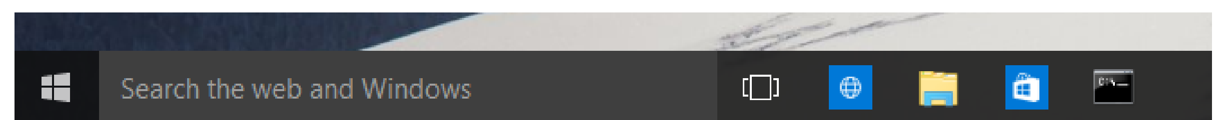


Figure 138 : Windows 10 : Barre de tâches

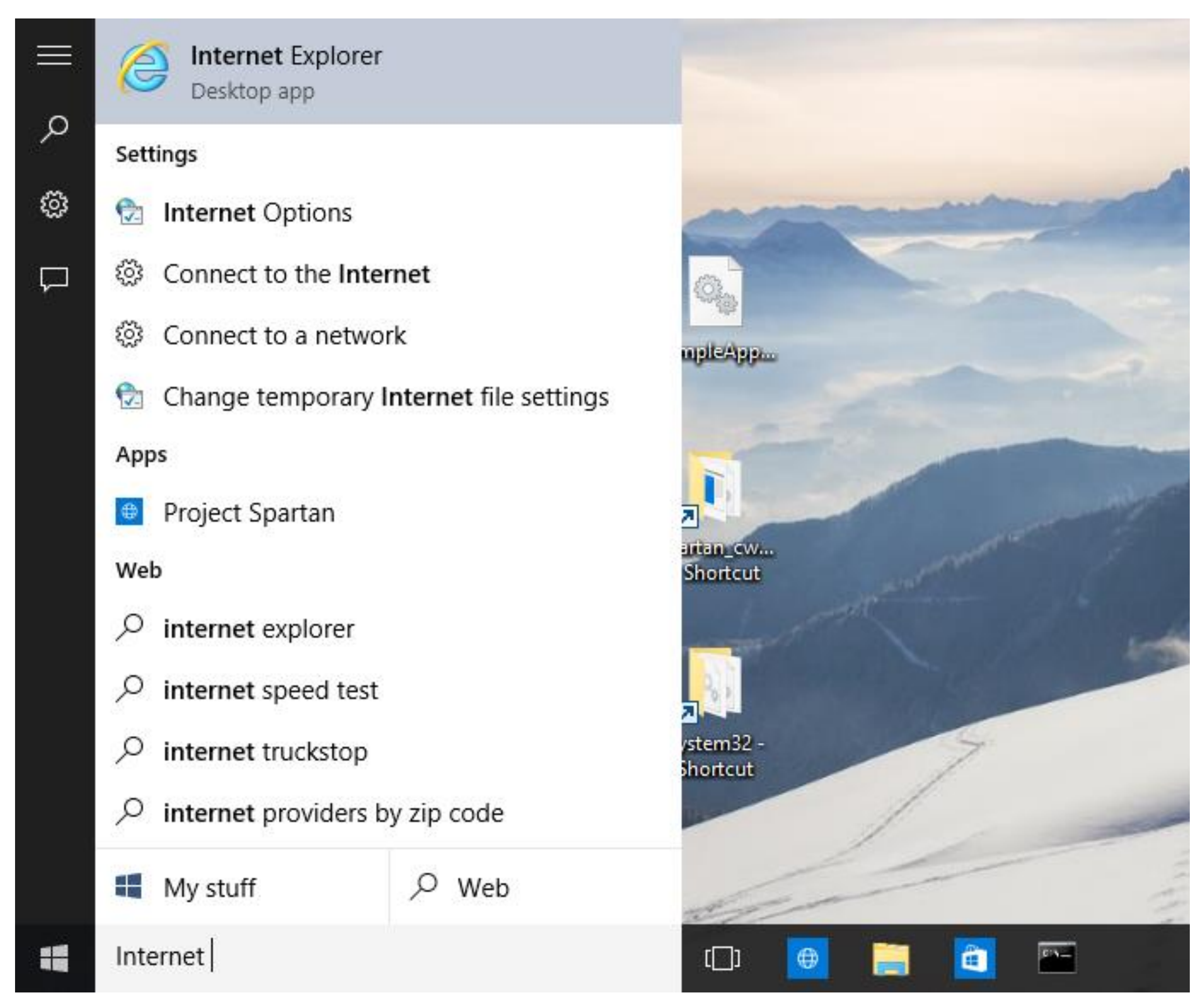


Figure 139 : Windows 10 : Recherche de « Internet Explorer »

Figure 140 : Windows 10 : Clic-droit sur le résultat « Internet Explorer » et choix de « ajouter à la barre de tâche »

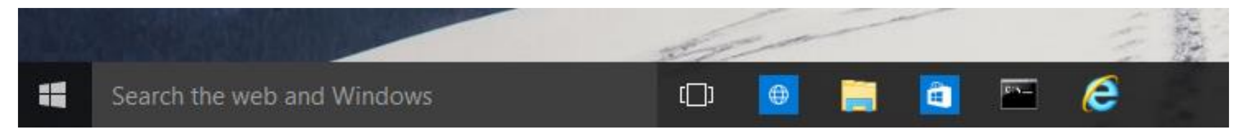


Figure 141 : Windows 10 : L'icône Internet Explorer apparaît dans la barre de tâche

38.3 Cryptolib CPS et Edge

Sous Edge, l'interface navigateur / carte CPS se fait exactement comme sous Internet Explorer, i.e. via le CSP.

La Cryptolib CPS v5 ne fonctionnait pas sous Edge du fait de l'utilisation d'APIs d'affichage de la boite de dialogue de saisie du code porteur rendues obsolètes sous la nouvelle architecture applicative promue par Microsoft (« Universal Apps »).

La Cryptolib CPS v5 a donc été corrigée en conséquence mais:

1. Une Cryptolib CPS v5 récente (> ou égale à 5.0.18 dont la sortie est prévue pour fin juillet 2015, en conjonction avec la sortie de Windows 10)
2. La Cryptolib CPS v5 64b doit être installée sur les postes Windows 10 64b
3. seuls les lecteurs PC/SC fonctionnent (en attente d'un GALSS 64b et de corrections dans le GALSS)

39Annexe – Table des figures

40Annexe – Liste des tableaux

41Notes

[fin du document]







Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
Tel : 01 58 45 32 50
esante.gouv.fr